



# FortiGate Log Message Reference

## v5.0 Patch Release 10



## FortiGate Log Message Reference - FortiOS 5.0.10

March 13, 2015

01-510-112804-20150313

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	<a href="https://docs.fortinet.com">docs.fortinet.com</a>
Knowledge Base	<a href="https://kb.fortinet.com">kb.fortinet.com</a>
Customer Service & Support	<a href="https://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="https://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="https://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

# Change Log

Date	Change Description
2013-03-20	Initial Release.
2013-09-27	Patch 4 Release.
2014-04-01	Patch 6 Release. Added Variable Event Logs Addendum.
2015-01-16	Patch 9 Release. Complete corrections of all terminology.
2015-03-13	Patch 10 Release. Added new Variable Event Logs.

### Log Field Name Changes in FortiOS 5.0

4.3	5
app_cat	appcat
app_list	applist
app_type	apptype
asset_id	assetid
asset_name	assetname
attack_id	attackid
attack_name	attackname
carrier_ep	carrierip
cat_desc	catdesc
class_desc	classdesc
conn-mode	connmode
content_type	contenttype
dec_spi	decspi
dir	direction
dir_disp	dirdisp
dlp_sensor	dlpsensor
dst	dstip
dst_country	dstcountry
dst_intf	dstintf
dst_port	dstport
enc_spi	encspi
end-date	enddate
esp_auth	espauth
esp_transform	esptransform
filter_type	filtertype
icmp_code	icmpcode
icmp_id	icmpid
icmp_type	icmptype
incident_serialno	incidentserialno
lan_in	lanin
lan_out	lanout
loc_ip	locip
loc_port	locport
local_ip	locip
log_id	logid
malform_data	malformdata
malform_desc	malformdesc
message	msg
message_type	messagetype
os_family	osfamily
os_gen	osgen
os_vendor	osvendor
out_intf	outintf
ovrd_id	ovrdid
ovrd_tbl	ovrdtbl
perip_drop	shaperperipdropbyte
perip_name	shaperperipname

4.3	5
pri	level
profile_group	profilegroup
profile_type	profiletype
quota_exceeded	quotaexceeded
quota_max	quotamax
quota_used	quotaused
rcvd	rcvdbyte
rcvd_pkt	rcvdpkt
rem_ip	remip
rem_port	remport
remote_ip	remip
req_type	reqtype
request_name	requestname
rule_data	ruledata
rule_type	ruletype
sent	sentbyte
sent_pkt	sentpkt
shaper_drop_rcvd	shaperdroprcvdbyte
shaper_drop_sent	shaperdropsentbyte
shaper_rcvd_name	shaperrcvdname
shaper_sent_name	shapersentname
src	srcip
src_country	srccountry
src_intf	srcintf
src_port	srcport
start-date	startdate
tran_disp	trandisp
tran_ip	tranip
tran_port	transport
tran_sip	transip
tran_sport	transport
url_type	urltype
urlfilter_idx	urlfilteridx
urlfilter_list	urlfilterlist
voip_proto	voippproto
vpn_tunnel	vpntunnel
vpn_type	vpntype
vuln_cat	vulncat
vuln_cnt	vulncnt
vuln_id	vulnid
vuln_ref	vulnref
wan_in	wanin
wan_out	wanout
wanopt_app_type	wanoptapptype
xauth_group	xauthgroup
xauth_user	xauthuser

# Log Subtype Name Changes in FortiOS 5.0

## 4.3 subtypes

## 5.0 subtypes

<b>traffic</b>	allowed	forward/local/multicast
	webcache-traffic, wanopt-traffic, explicit-proxy-traffic	forward
	failed-conn, violation, other	forward

<b>event</b>	ipsec, sslvpn-user, sslvpn-admin, sslvpn-session	vpn
	ha, gtp, nac-quarantine, config, notification, perf-historical, forticlient, mms-stats, amc-intf-bypass, admin, ldb-monitor, pattern	system
	dns, dhcp, l2tp/pptp/pppoe	router
	auth, radius	user
	wireless	wireless
	wad	wad
	voip	moved to voip logs section

<b>virus</b>	infected	infected
	filename	filename
	oversize	oversized
	scanerror	scanerror
	-----	analytics
	-----	switchproto

<b>webfilter</b>	content	content
	urlfilter	urlfilter
	ftgd_blk	ftgd_blk
	ftgd_allow	ftgd_allow
	ftgd_err	ftgd_err
	activexfilter	activexfilter
	cookiefilter	cookiefilter
	appletfilter	appletfilter
	ftgd_quota_counting	ftgd_quota_counting
	ftgd_quota	ftgd_quota
	-----	ftgd_quota_expired
	-----	webfilter_command_block

<b>ips</b>	signature	signature
	anomaly	anomaly
<b>emailfilter</b>	msn-hotmail	msn
	yahoo-mail	yahoo
	smtp	smtp
	pop3	pop3
	imap	imap
	carrier-endpoint-filter	endpointfilter
	mass-mms	mms
	-----	google
	-----	mapi

<b>netscan</b>	discovery	discovery
	vulnerability	vulnerability

<b>dlp</b>	dlp	dlp
	-----	dlp-docsource

<b>app-ctrl</b>	app-ctrl-all	app-ctrl-all
-----------------	--------------	--------------

<b>content</b>	http	http
	ftp	ftp
	smtp	smtp
	pop3	pop3
	imap	imap
	https	https
	im-all	im-all
	nntp	nntp
	voip	voip
	mm1	mm1
	mm3	mm3
	mm4	mm4
	mm7	mm7
	smtps	smtps
	pop3s	pop3s
	imaps	imaps

<b>voip</b>	-----	voip
-------------	-------	------



# Traffic

## 2

**Message ID:** 000002

**Message Description:** allowed message

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
type	traffic
subtype	forward
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
status	The status of the traffic.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
trandisp	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
tranip	The translated IP in NAT mode. For Transparent mode, it is zero.
tranport	The translated port number in NAT mode. For Transparent mode, it is zero.
transip	The translated source IP in NAT mode. For Transparent mode, it is zero.
transport	The translated source port number in NAT mode. For Transparent mode, it is zero.
service	The service where the event or activity occurred.
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
duration	Time value in seconds.



<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

### 3

**Message ID:** 000003

**Message Description:** violation message

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** warning

Log field	Meaning
type	traffic
subtype	invalid
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
status	The status of the traffic.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
service	The service where the event or activity occurred.
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
duration	Time value in seconds.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sentbyte	The number of sent bytes related to the log message.
rcvdbyte	The number of received bytes related to the log message.
shaperdropsentbyte	Shaper dropped sent bytes.
shaperdroprcvdbyte	Shaper dropped received bytes.
shaperperipdropbyte	PerIP dropped bytes.

<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 4

**Message ID:** 000004

**Message Description:** other message

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** notice

Log field	Meaning
type	traffic
subtype	invalid
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
status	The status of the traffic.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
tranip	The translated IP in NAT mode. For Transparent mode, it is zero.
tranport	The translated port number in NAT mode. For Transparent mode, it is zero.
transip	The translated source IP in NAT mode. For Transparent mode, it is zero.
transport	The translated source port number in NAT mode. For Transparent mode, it is zero.
service	The service where the event or activity occurred.
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
duration	Time value in seconds.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sentbyte	The number of sent bytes related to the log message.

<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 5

**Message ID:** 000005

**Message Description:** allowed icmp message

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	invalid
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>trandisp</b>	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>tranip</b>	The translated IP in NAT mode. For Transparent mode, it is zero.
<b>tranport</b>	The translated port number in NAT mode. For Transparent mode, it is zero.
<b>transip</b>	The translated source IP in NAT mode. For Transparent mode, it is zero.
<b>transport</b>	The translated source port number in NAT mode. For Transparent mode, it is zero.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.

<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 6

**Message ID:** 000006

**Message Description:** deny internal icmp message

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	invalid
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.



<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 7

**Message ID:** 000007

**Message Description:** deny external icmp message

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** warning

Log field	Meaning
type	traffic
subtype	invalid
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
status	The status of the traffic.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
service	The service where the event or activity occurred.
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
duration	Time value in seconds.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sentbyte	The number of sent bytes related to the log message.
rcvdbyte	The number of received bytes related to the log message.
shaperdropsentbyte	Shaper dropped sent bytes.
shaperdroprcvdbyte	Shaper dropped received bytes.
shaperperipdropbyte	PerIP dropped bytes.

<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 8

**Message ID:** 000008

**Message Description:** WAN optimization traffic

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	forward
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>wanoptapptype</b>	WANOpt app type. One of: <i>web-cache</i> , <i>cifs</i> , <i>tcp</i> , <i>ftp</i> , <i>mapi</i> , <i>http</i> , <i>web-proxy</i> , <i>ftp-proxy</i> .
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>wanin</b>	WAN in.
<b>wanout</b>	WAN out.
<b>lanin</b>	LAN in.
<b>lanout</b>	LAN out.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.

<b>unauthusersource</b>	Method used to detect username.
-------------------------	---------------------------------

# 9

**Message ID:** 000009

**Message Description:** webcache traffic

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	forward
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>wanoptapptype</b>	WANOpt app type. One of: <i>web-cache</i> , <i>cifs</i> , <i>tcp</i> , <i>ftp</i> , <i>mapi</i> , <i>http</i> , <i>web-proxy</i> , <i>ftp-proxy</i> .
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>wanin</b>	WAN in.
<b>wanout</b>	WAN out.
<b>lanin</b>	LAN in.
<b>lanout</b>	LAN out.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.

<b>unauthusersource</b>	Method used to detect username.
-------------------------	---------------------------------

# 10

**Message ID:** 000010

**Message Description:** explicit proxy traffic

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
type	traffic
subtype	forward
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
wanoptapptype	WANOpt app type. One of: <i>web-cache</i> , <i>cifs</i> , <i>tcp</i> , <i>ftp</i> , <i>mapi</i> , <i>http</i> , <i>web-proxy</i> , <i>ftp-proxy</i> .
duration	Time value in seconds.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
wanin	WAN in.
wanout	WAN out.
lanin	LAN in.
lanout	LAN out.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.



<b>unauthusersource</b>	Method used to detect username.
-------------------------	---------------------------------

# 11

**Message ID:** 000011

**Message Description:** failed connection attempts

**Type (type):** traffic

**Subtype (subtype):** invalid

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	invalid
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 12

**Message ID:** 000012

**Message Description:** multicast allowed message

**Type (type):** traffic

**Subtype (subtype):** multicast

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	multicast
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>trandisp</b>	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>tranip</b>	The translated IP in NAT mode. For Transparent mode, it is zero.
<b>tranport</b>	The translated port number in NAT mode. For Transparent mode, it is zero.
<b>transip</b>	The translated source IP in NAT mode. For Transparent mode, it is zero.
<b>transport</b>	The translated source port number in NAT mode. For Transparent mode, it is zero.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.

<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 13

**Message ID:** 000013

**Message Description:** traffic forward message

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	forward
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>trandisp</b>	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>tranip</b>	The translated IP in NAT mode. For Transparent mode, it is zero.
<b>tranport</b>	The translated port number in NAT mode. For Transparent mode, it is zero.
<b>transip</b>	The translated source IP in NAT mode. For Transparent mode, it is zero.
<b>transport</b>	The translated source port number in NAT mode. For Transparent mode, it is zero.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.

<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>utmaction</b>	The UTM action taken by the system.
<b>filename</b>	The name of the file that was transferred.
<b>virus</b>	The name of the virus detected.
<b>attack</b>	ATTACK
<b>hostname</b>	The hostname information.
<b>catdesc</b>	The category description.
<b>sender</b>	SENDER
<b>recipient</b>	RECIPIENT
<b>mailcount</b>	MAILCOUNT

<b>spamcount</b>	SPAMCOUNT
<b>dlprule</b>	DLP rule.
<b>utmevent</b>	The type of UTM event taking place.
<b>utmseverity</b>	UTM severity.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 14

**Message ID:** 000014

**Message Description:** traffic local message

**Type (type):** traffic

**Subtype (subtype):** local

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	local
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>trandisp</b>	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>tranip</b>	The translated IP in NAT mode. For Transparent mode, it is zero.
<b>tranport</b>	The translated port number in NAT mode. For Transparent mode, it is zero.
<b>transip</b>	The translated source IP in NAT mode. For Transparent mode, it is zero.
<b>transport</b>	The translated source port number in NAT mode. For Transparent mode, it is zero.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.



<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 15

**Message ID:** 000015

**Message Description:** start forward message

**Type (type):** traffic

**Subtype (subtype):** forward

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	traffic
<b>subtype</b>	forward
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>status</b>	The status of the traffic.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>trandisp</b>	Whether the packet is source NAT translated ( <i>snat</i> ) or destination NAT translated ( <i>dnat</i> ), both ( <i>snat+dnat</i> ) or neither ( <i>noop</i> ).
<b>srcip</b>	The source IP.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstname</b>	The destination name. This can be a name or an IP address.
<b>dstcountry</b>	Destination country.
<b>srccountry</b>	Source country.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>tranip</b>	The translated IP in NAT mode. For Transparent mode, it is zero.
<b>tranport</b>	The translated port number in NAT mode. For Transparent mode, it is zero.
<b>transip</b>	The translated source IP in NAT mode. For Transparent mode, it is zero.
<b>transport</b>	The translated source port number in NAT mode. For Transparent mode, it is zero.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>duration</b>	Time value in seconds.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.

<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# 16

**Message ID:** 000016

**Message Description:** start local message

**Type (type):** traffic

**Subtype (subtype):** local

**Level/Severity:** notice

Log field	Meaning
type	traffic
subtype	local
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
status	The status of the traffic.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstname	The destination name. This can be a name or an IP address.
dstcountry	Destination country.
srccountry	Source country.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
tranip	The translated IP in NAT mode. For Transparent mode, it is zero.
tranport	The translated port number in NAT mode. For Transparent mode, it is zero.
transip	The translated source IP in NAT mode. For Transparent mode, it is zero.
transport	The translated source port number in NAT mode. For Transparent mode, it is zero.
service	The service where the event or activity occurred.
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
duration	Time value in seconds.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sentbyte	The number of sent bytes related to the log message.

<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>shaperdropsentbyte</b>	Shaper dropped sent bytes.
<b>shaperdroprcvdbyte</b>	Shaper dropped received bytes.
<b>shaperperipdropbyte</b>	PerIP dropped bytes.
<b>shapersentname</b>	The name of the traffic shaper sending the bytes.
<b>shaperrcvdname</b>	The name of the traffic shaper receiving the bytes.
<b>shaperperipname</b>	The perIP shaper name.
<b>sentpkt</b>	The number of sent packets related to the log message.
<b>rcvdpkt</b>	The number of received packets related to the log message.
<b>vpn</b>	The name of the VPN tunnel used by the traffic.
<b>vpntype</b>	The type of VPN tunnel that the traffic is flowing through. This field can be any one of the following: <i>ipsec-static</i> , <i>ipsec-dynamic</i> , <i>ipsec-ddns</i> , <i>sslvpn</i> .
<b>vpntunnel</b>	The name of the VPN tunnel that was used. For example, <i>ssl_vpn1</i> .
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>sessionid</b>	Session ID.
<b>appid</b>	Application ID.
<b>app</b>	The name of the application that triggered the action within the control list. For example, <i>SSL</i> .
<b>appcat</b>	The application category that the application is associated with.
<b>applist</b>	The name of the application control list that was used to detect and take action.
<b>appact</b>	Application action.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>crscore</b>	Client Reputation score.
<b>craction</b>	Client Reputation action.

# Netscan

## 4096

**Message ID:** 004096

**Message Description:** Network scan performed

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** vulnerability

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	vulnerability
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>start</b>	GMT epoch time the scan started.
<b>end</b>	GMT epoch time the scan ended.
<b>status</b>	Scan status: <i>start, stop, pause, resume, complete.</i>
<b>engine</b>	Version of the netscan engine.
<b>plugin</b>	Version of the netscan plugin.

# 4097

**Message ID:** 004097

**Message Description:** Network scan performed

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	discovery
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>start</b>	GMT epoch time the scan started.
<b>end</b>	GMT epoch time the scan ended.
<b>status</b>	Scan status: <i>start, stop, pause, resume, complete.</i>
<b>engine</b>	Version of the netscan engine.
<b>plugin</b>	Version of the netscan plugin.

# 4098

**Message ID:** 004098

**Message Description:** Netscan vulnerability detected

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** vulnerability

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	vulnerability
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>dstip</b>	The destination IP.
<b>vuln</b>	Name of the detected vulnerability.
<b>vulncat</b>	Category of the detected vulnerability.
<b>vulnid</b>	ID of the detected vulnerability.
<b>vulnref</b>	Reference to the detected vulnerability in FortiGuard.
<b>severity</b>	The priority level of the attack log. Can be <i>info, low, medium, high, or critical.</i>
<b>vulnscore</b>	NIST score of the detected vulnerability.
<b>proto</b>	Protocol. Either <i>TCP</i> or <i>UDP</i> .
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.



# 4099

**Message ID:** 004099

**Message Description:** Nmap OS detected

**Type (type):** utm

**Subtype (subtype):** nmap

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	nmap
eventtype	discovery
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
action	The nature of the nmap event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
dstip	The destination IP.
os	Operating system name.
osfamily	OS family.
osgen	OS generation.
osvendor	OS vendor.

# 4100

**Message ID:** 004100

**Message Description:** Nmap service detected

**Type (type):** utm

**Subtype (subtype):** nmap

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	nmap
<b>eventtype</b>	discovery
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the nmap event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>dstip</b>	The destination IP.
<b>service</b>	The service where the event or activity occurred.
<b>proto</b>	Protocol. Either <i>TCP</i> or <i>UDP</i> .
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.

# 4101

**Message ID:** 004101

**Message Description:** Notification message

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** vulnerability

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	vulnerability
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>

# 4102

**Message ID:** 004102

**Message Description:** Notification message

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	discovery
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>

# 4103

**Message ID:** 004103

**Message Description:** Netscan number of vulnerabilities detected

**Type (type):** utm

**Subtype (subtype):** netscan

**Event Type (eventtype):** vulnerability

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	netscan
<b>eventtype</b>	vulnerability
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the netscan event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>dstip</b>	The destination IP.
<b>vulncnt</b>	Vulnerability count.

# 4104

**Message ID:** 004104

**Message Description:** Nmap host detected

**Type (type):** utm

**Subtype (subtype):** nmap

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	nmap
eventtype	discovery
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
action	The nature of the nmap event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
dstip	The destination IP.
method	The method information.
assetid	Asset ID for this host.
assetname	Asset definition for this host.

# 4105

**Message ID:** 004105

**Message Description:** Nmap port detected

**Type (type):** utm

**Subtype (subtype):** nmap

**Event Type (eventtype):** discovery

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	nmap
<b>eventtype</b>	discovery
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>action</b>	The nature of the nmap event. <i>Scan, vuln-detection, host-detection, os-scan, port-detection, service-detection, vuln-count.</i>
<b>dstip</b>	The destination IP.
<b>proto</b>	Protocol. Either <i>TCP</i> or <i>UDP</i> .
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.

# Virus

## 8192

**Message ID:** 008192

**Message Description:** virus infected block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	virus
eventtype	infected
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
direction	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
file	The name of the file.
checksum	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.



<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.
<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File is infected."

# 8193

**Message ID:** 008193

**Message Description:** virus infected pass

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File is infected."

# 8194

**Message ID:** 008194

**Message Description:** virus infected mime block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File is infected."

# 8195

**Message ID:** 008195

**Message Description:** virus infected mime pass

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File submitted to FortiGuard Analytics."

# 8196

**Message ID:** 008196

**Message Description:** virus infected worm block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	virus
eventtype	infected
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
virus	The name of the virus detected.
dtype	Dtype.
url	The URL address.
profile	The name of the profile that was used to detect and take action.
profiletype	The type of profile responsible for the UTM action taken.
user	User name.
group	The group name.



<b>msg</b>	"Worm detected."
------------	------------------

# 8197

**Message ID:** 008197

**Message Description:** virus infected worm monitor

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.

<b>msg</b>	"Worm detected."
------------	------------------

# 8198

**Message ID:** 008198

**Message Description:** virus infected worm mime block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.

<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Worm detected."

# 8199

**Message ID:** 008199

**Message Description:** virus infected worm mime monitor

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.

<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Worm detected."

# 8448

**Message ID:** 008448

**Message Description:** virus blocked (warning)

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	filename
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>filefilter</b>	The filter used to identify the affected file.
<b>filetype</b>	The filetype of the affected file.
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).



<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is blocked."

# 8449

**Message ID:** 008449

**Message Description:** virus blocked (notice)

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	filename
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>filefilter</b>	The filter used to identify the affected file.
<b>filetype</b>	The filetype of the affected file.
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).

<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is blocked."

# 8450

**Message ID:** 008450

**Message Description:** virus blocked mime (warning)

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	filename
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>filefilter</b>	The filter used to identify the affected file.
<b>filetype</b>	The filetype of the affected file.
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).

<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is blocked."

# 8451

**Message ID:** 008451

**Message Description:** virus blocked mime (notice)

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	filename
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>filefilter</b>	The filter used to identify the affected file.
<b>filetype</b>	The filetype of the affected file.
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).

<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is blocked."

# 8452

**Message ID:** 008452

**Message Description:** virus blocked command

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	virus
eventtype	filename
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
url	The URL address.
user	User name.
group	The group name.
command	Command information.
agent	Agent.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.



msg	"Command blocked."
-----	--------------------

# 8453

**Message ID:** 008453

**Message Description:** virus intercepted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	virus
eventtype	filename
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
direction	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
filefilter	The filter used to identify the affected file.
filetype	The filetype of the affected file.
file	The name of the file.
checksum	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
quarskip	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).

<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is intercepted."

# 8454

**Message ID:** 008454

**Message Description:** virus intercepted mime

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	filename
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>filefilter</b>	The filter used to identify the affected file.
<b>filetype</b>	The filetype of the affected file.
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).

<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File is intercepted."

# 8455

**Message ID:** 008455

**Message Description:** virus exempted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	virus
eventtype	filename
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
direction	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
filefilter	The filter used to identify the affected file.
filetype	The filetype of the affected file.
file	The name of the file.
url	The URL address.
profile	The name of the profile that was used to detect and take action.
profiletype	The type of profile responsible for the UTM action taken.

<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File has been exempted."

# 8456

**Message ID:** 008456

**Message Description:** virus exempted mime

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** filename

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	virus
eventtype	filename
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
status	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
service	The service where the event or activity occurred.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
direction	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
filefilter	The filter used to identify the affected file.
filetype	The filetype of the affected file.
file	The name of the file.
url	The URL address.
profile	The name of the profile that was used to detect and take action.
profiletype	The type of profile responsible for the UTM action taken.



<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"File has been exempted."

# 8457

**Message ID:** 008457

**Message Description:** mms content checksum

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A, TX, or RX</i> .
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.

<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Blocked by MMS content checksum."

# 8458

**Message ID:** 008458

**Message Description:** mms content checksum

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** infected

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	infected
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A, TX, or RX</i> .
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>file</b>	The name of the file.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.

<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Matched by MMS content checksum."

# 8704

**Message ID:** 008704

**Message Description:** oversized block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** oversize

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	oversize
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>file</b>	The name of the file.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.

<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Size limit exceeded."

# 8705

**Message ID:** 008705

**Message Description:** oversized pass

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** oversize

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	oversize
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>file</b>	The name of the file.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>agent</b>	Agent.



<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>msg</b>	"Size limit exceeded."

# 8706

**Message ID:** 008706

**Message Description:** oversized mime block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** oversize

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	oversize
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>file</b>	The name of the file.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>from</b>	Source identifier.

<b>to</b>	Destination identifier.
<b>msg</b>	"Size limit exceeded."

# 8707

**Message ID:** 008707

**Message Description:** oversized mime pass

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** oversize

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	oversize
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>file</b>	The name of the file.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>from</b>	Source identifier.

<b>to</b>	Destination identifier.
<b>msg</b>	"Size limit exceeded."

# 8720

**Message ID:** 008720

**Message Description:** switching protocols block

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** switchproto

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	switchproto
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.

<b>agent</b>	Agent.
<b>switchproto</b>	Protocol change information.
<b>msg</b>	"Switching protocols request."

# 8721

**Message ID:** 008721

**Message Description:** switching protocols bypass

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** switchproto

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	switchproto
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked, passthrough, monitored, analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.



<b>agent</b>	Agent.
<b>switchproto</b>	Protocol change information.
<b>msg</b>	"Switching protocols request."

# 8960

**Message ID:** 008960

**Message Description:** uncompressed nested limit reached

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File reached uncompressed nested limit."

# 8961

**Message ID:** 008961

**Message Description:** uncompressed size limit reached

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"File reached uncompressed size limit."

# 8962

**Message ID:** 008962

**Message Description:** archive is encrypted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Encrypted archive."

# 8963

**Message ID:** 008963

**Message Description:** archive is encrypted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.



<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Encrypted archive."

# 8964

**Message ID:** 008964

**Message Description:** archive is corrupted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Corrupted archive."

# 8965

**Message ID:** 008965

**Message Description:** archive is corrupted

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Corrupted archive."

# 8966

**Message ID:** 008966

**Message Description:** multipart archive

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Multipart archive."

# 8967

**Message ID:** 008967

**Message Description:** multipart archive

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.



<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Multipart archive."

# 8968

**Message ID:** 008968

**Message Description:** nested archive

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Nested archive."

# 8969

**Message ID:** 008969

**Message Description:** nested archive

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Nested archive."

# 8970

**Message ID:** 008970

**Message Description:** archive is oversized

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Oversized archive."

# 8971

**Message ID:** 008971

**Message Description:** archive is oversized

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.



<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Oversized archive."

# 8972

**Message ID:** 008972

**Message Description:** unhandled archive type

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Unhandled archive."

# 8973

**Message ID:** 008973

**Message Description:** unhandled archive type

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** scanerror

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	scanerror
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	"Unhandled archive."

# 9233

**Message ID:** 009233

**Message Description:** FortiGuard analytics

**Type (type):** utm

**Subtype (subtype):** virus

**Event Type (eventtype):** analytics

**Level/Severity:** notice

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	virus
<b>eventtype</b>	analytics
<b>level</b>	notice
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>status</b>	The status of the virus or packet: <i>blocked</i> , <i>passthrough</i> , <i>monitored</i> , <i>analytics</i> .
<b>service</b>	The service where the event or activity occurred.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>file</b>	The name of the file.
<b>checksum</b>	The checksum of the file that was scanned by the FortiGate unit. If two files have different names but the same checksum, the FortiGate unit assumes that they have the same content.
<b>quarskip</b>	Quarantine skip explanation: <i>notskip</i> (file quarantined), <i>filepattern</i> (not quarantined due to HTTP GET file pattern block), <i>oversized</i> (not quarantined due to no oversize rule), <i>unknown</i> (not quarantined for other reason).
<b>virus</b>	The name of the virus detected.
<b>dtype</b>	Dtype.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>url</b>	The URL address.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>sha256</b>	SHA256 hash.
<b>analyticssubmit</b>	Whether analytics were submitted or not. Can be <i>false</i> or <i>true</i> .
<b>msg</b>	

# Webfilter

## 12288

**Message ID:** 012288

**Message Description:** Web content banned word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .



<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>banword</b>	Banned word flagged in the message.
<b>msg</b>	"URL was blocked because it contained banned word(s)."

# 12289

**Message ID:** 012289

**Message Description:** Web content MMS banned word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>banword</b>	Banned word flagged in the message.
<b>msg</b>	"Message was blocked because it contained banned word(s)."

# 12290

**Message ID:** 012290

**Message Description:** Web content exempt word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>banword</b>	Banned word flagged in the message.
<b>msg</b>	"URL was exempted because it contained exempt word(s)."

# 12291

**Message ID:** 012291

**Message Description:** Web content MMS exempt word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>banword</b>	Banned word flagged in the message.
<b>msg</b>	"Message was exempted because it contained exempt word(s)."

# 12292

**Message ID:** 012292

**Message Description:** Web search key word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.



<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>keyword</b>	Flagged or searched keyword.
<b>msg</b>	"Message contained a key word in the profile list."

# 12293

**Message ID:** 012293

**Message Description:** Web search

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>keyword</b>	Flagged or searched keyword.
<b>msg</b>	"Search phrase detected."

# 12305

**Message ID:** 012305

**Message Description:** Web content MMS banned word

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>direction</b>	Message direction. One of: <i>N/A</i> , <i>TX</i> , or <i>RX</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>banword</b>	Banned word flagged in the message.
<b>msg</b>	"Message was logged because it contained a banned word."

# 12544

**Message ID:** 012544

**Message Description:** URL filter block

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
urlfilteridx	URL filter index.
urlfilterlist	URL filter list name.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.

<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"URL was blocked because it is in the URL filter list."

# 12545

**Message ID:** 012545

**Message Description:** URL filter exempt

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
urlfilteridx	URL filter index.
urlfilterlist	URL filter list name.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.



<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"URL was exempted because it is in the URL filter list."

# 12546

**Message ID:** 012546

**Message Description:** URL filter allow

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
urlfilteridx	URL filter index.
urlfilterlist	URL filter list name.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.

<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"URL was allowed because it is in the URL filter list."

# 12547

**Message ID:** 012547

**Message Description:** URL filter invalid hostname (Block/HTTP)

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
hostname	The hostname information.
status	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
reqtype	The request type, either <i>direct</i> or <i>referral</i> .
sentbyte	The number of sent bytes related to the log message.

<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"The HTTP request contained an invalid domain name."

# 12548

**Message ID:** 012548

**Message Description:** URL filter invalid hostname (Block/HTTPS)

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
hostname	The hostname information.
status	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
reqtype	The request type, either <i>direct</i> or <i>referral</i> .
sentbyte	The number of sent bytes related to the log message.

<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"The certificate for the HTTPS session contained an invalid domain name."

# 12549

**Message ID:** 012549

**Message Description:** URL filter invalid hostname (Filter/HTTP)

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
hostname	The hostname information.
status	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
reqtype	The request type, either <i>direct</i> or <i>referral</i> .
sentbyte	The number of sent bytes related to the log message.



<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"The HTTP request contained an invalid domain name. The session has been filtered by IP only."

# 12550

**Message ID:** 012550

**Message Description:** URL filter invalid hostname (Filter/HTTPS)

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
hostname	The hostname information.
status	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
reqtype	The request type, either <i>direct</i> or <i>referral</i> .
sentbyte	The number of sent bytes related to the log message.

<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"The certificate for this HTTPS session contained an invalid domain name. The session has been filtered by IP only."

# 12553

**Message ID:** 012553

**Message Description:** Server certificate validation failed

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
sentbyte	The number of sent bytes related to the log message.
rcvdbyte	The number of received bytes related to the log message.
msg	"The server certificate validation failed."

# 12554

**Message ID:** 012554

**Message Description:** Unknown SSL session ID

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
service	The service where the event or activity occurred.
status	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
sentbyte	The number of sent bytes related to the log message.
rcvbyte	The number of received bytes related to the log message.
msg	"The SSL session was blocked because the session ID was unknown."

# 12555

**Message ID:** 012555

**Message Description:** SSL session blocked due to invalid/missing server certificate

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
service	The service where the event or activity occurred.
status	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
sentbyte	The number of sent bytes related to the log message.
rcvbyte	The number of received bytes related to the log message.
msg	"The SSL session was blocked because the server certificate was missing or invalid."

# 12556

**Message ID:** 012556

**Message Description:** SSL session ignored due to invalid/missing server certificate

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
profiletype	The type of profile responsible for the UTM action taken.
profile	The name of the profile that was used to detect and take action.
service	The service where the event or activity occurred.
status	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
sentbyte	The number of sent bytes related to the log message.
rcvbyte	The number of received bytes related to the log message.
msg	"The SSL session was ignored because the server certificate was missing or invalid."

# 12557

**Message ID:** 012557

**Message Description:** FortiGuard service inactive

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** critical

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	critical
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
msg	"FortiGuard is enabled in the protection profile but the FortiGuard service is not enabled."



# 12558

**Message ID:** 012558

**Message Description:** Rating error occurs

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	webfilter
<b>eventtype</b>	urlfilter
<b>level</b>	information
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>user</b>	User name.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>urltype</b>	URL type. One of: <i>HTTP, HTTPS, FTP, Telnet, mail, phishing</i> .
<b>hostname</b>	The hostname information.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>error</b>	Error.
<b>url</b>	The URL address.
<b>msg</b>	"Policy allows URLs when a rating error occurs."

# 12559

**Message ID:** 012559

**Message Description:** URL filter pass

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
urlfilteridx	URL filter index.
urlfilterlist	URL filter list name.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.

<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"URL was passed because it is in the URL filter list."

# 12800

**Message ID:** 012800

**Message Description:** FortiGuard webfilter error

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_err

**Level/Severity:** error

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_err
level	error
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>error</b>	Error.
<b>msg</b>	"A rating error occurred."

# 12801

**Message ID:** 012801

**Message Description:** FortiGuard webfilter error

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_err

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_err
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>error</b>	Error.
<b>msg</b>	"A rating error occurred."

# 12802

**Message ID:** 012802

**Message Description:** Daily fortiguard quota status

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_quota

**Level/Severity:** information

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	webfilter
<b>eventtype</b>	ftgd_quota
<b>level</b>	information
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>quotaexceeded</b>	Quota exceeded: <i>yes</i> or <i>no</i> .
<b>quotatype</b>	The quota type, either: <i>time</i> or <i>traffic</i> .
<b>quotaused</b>	Quota time used (in seconds).
<b>quotamax</b>	Maximum quota time allowed (in seconds).
<b>catdesc</b>	The category description.
<b>user</b>	User name.
<b>profile</b>	The name of the profile that was used to detect and take action.



# 13056

**Message ID:** 013056

**Message Description:** FortiGuard webfilter category block

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_blk

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_blk
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>msg</b>	"URL belongs to a denied category in policy."

# 13057

**Message ID:** 013057

**Message Description:** FortiGuard webfilter category block

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_blk

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_blk
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>msg</b>	"URL belongs to a category with warnings enabled."

# 13312

**Message ID:** 013312

**Message Description:** FortiGuard webfilter category allow

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_allow

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_allow
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>msg</b>	"URL belongs to a allowed category in policy."

# 13313

**Message ID:** 013313

**Message Description:** FortiGuard webfilter allow

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_allow

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_allow
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>mode</b>	Mode.
<b>ruletype</b>	Rule type. One of: <i>Directory, domain, rating, unhandled.</i>
<b>ruledata</b>	Rule data.
<b>ovrdtbl</b>	Override table name.
<b>ovrddid</b>	Override ID.
<b>msg</b>	"URL belongs to an override rule."



# 13314

**Message ID:** 013314

**Message Description:** FortiGuard webfilter allow

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_allow

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_allow
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>mode</b>	Mode.
<b>ruletype</b>	Rule type. One of: <i>Directory, domain, rating, unhandled.</i>
<b>ruledata</b>	Rule data.
<b>ovrdtbl</b>	Override table name.
<b>ovrddid</b>	Override ID.
<b>msg</b>	"URL belongs to an override rule."

# 13315

**Message ID:** 013315

**Message Description:** FortiGuard webfilter category quota counting

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** ftgd\_quota\_counting

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	ftgd_quota_counting
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>quotatype</b>	The quota type, either: <i>time</i> or <i>traffic</i> .
<b>quotaused</b>	Quota time used (in seconds).
<b>quotamax</b>	Maximum quota time allowed (in seconds).
<b>msg</b>	"Webfilter quota has begun counting."

# 13316

**Message ID:** 013316

**Message Description:** FortiGuard webfilter category quota expired

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>quotatype</b>	The quota type, either: <i>time</i> or <i>traffic</i> .
<b>quotaused</b>	Quota time used (in seconds).
<b>quotamax</b>	Maximum quota time allowed (in seconds).
<b>msg</b>	"Webfilter quota for category has expired."

# 13317

**Message ID:** 013317

**Message Description:** URL visited

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** urlfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	urlfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP</i> .
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>method</b>	The method information.
<b>class</b>	The class.
<b>classdesc</b>	The class description.
<b>cat</b>	The category.
<b>catdesc</b>	The category description.
<b>msg</b>	"URL has been visited."



# 13568

**Message ID:** 013568

**Message Description:** Web script filter ActiveX

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** activexfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	activexfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>count</b>	Number of packets.
<b>msg</b>	"ActiveX script was removed."

# 13573

**Message ID:** 013573

**Message Description:** Web script filter cookie

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** cookiefilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	cookiefilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>msg</b>	"Cookie was removed."

# 13584

**Message ID:** 013584

**Message Description:** Web script filter applet

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** appletfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	appletfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>count</b>	Number of packets.
<b>msg</b>	"Java applet was removed."

# 13601

**Message ID:** 013601

**Message Description:** Web cookie filter

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** cookiefilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	cookiefilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>count</b>	Number of packets.
<b>filtertype</b>	The script filter type. Can be: <i>N/A, jscript, javascript, vbscript, or unknown.</i>
<b>msg</b>	"Cookie was removed entirely."



# 13602

**Message ID:** 013602

**Message Description:** Web referer filter

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** cookiefilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	webfilter
eventtype	cookiefilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>status</b>	The status of the traffic: <i>blocked, exempted, allowed, passthrough, filtered, DLP.</i>
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>count</b>	Number of packets.
<b>filtertype</b>	The script filter type. Can be: <i>N/A, jscript, javascript, vbscript, or unknown.</i>
<b>msg</b>	"Referer was removed from request."

# 13603

**Message ID:** 013603

**Message Description:** Command blocked

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** webfilter\_command\_block

**Level/Severity:** warning

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	webfilter
<b>eventtype</b>	webfilter_command_block
<b>level</b>	warning
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>custom</b>	Custom field.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>sessionid</b>	Session ID.
<b>initiator</b>	The initiator name.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcip</b>	The source IP.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstip</b>	The destination IP.
<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>hostname</b>	The hostname information.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>service</b>	The service where the event or activity occurred.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .

<b>msg</b>	"Command blocked."
------------	--------------------

# 13616

**Message ID:** 013616

**Message Description:** Content type blocked

**Type (type):** utm

**Subtype (subtype):** webfilter

**Event Type (eventtype):** content

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	webfilter
eventtype	content
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
initiator	The initiator name.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.

<b>hostname</b>	The hostname information.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>reqtype</b>	The request type, either <i>direct</i> or <i>referral</i> .
<b>url</b>	The URL address.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>status</b>	The status of the traffic: <i>blocked</i> , <i>exempted</i> , <i>allowed</i> , <i>passthrough</i> , <i>filtered</i> , <i>DLP</i> .
<b>agent</b>	Agent.
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>contenttype</b>	Content type.
<b>msg</b>	"Blocked by HTTP Header Content Type."

# IPS

## 16384

**Message ID:** 016384

**Message Description:** attack signature (tcp/udp)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** signature

**Level/Severity:** alert

Log field	Meaning
<b>type</b>	utm
<b>subtype</b>	ips
<b>eventtype</b>	signature
<b>level</b>	alert
<b>date</b>	The date at which the log was recorded.
<b>time</b>	The time at which the log was recorded.
<b>severity</b>	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
<b>srcip</b>	The source IP.
<b>dstip</b>	The destination IP.
<b>srcintf</b>	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
<b>dstintf</b>	The destination interface.
<b>policyid</b>	The ID number of the firewall policy that applies to the session or packet.
<b>indentidx</b>	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
<b>custom</b>	Custom field.
<b>sessionid</b>	Session ID.
<b>status</b>	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
<b>proto</b>	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
<b>service</b>	The service where the event or activity occurred.
<b>vd</b>	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
<b>count</b>	Number of packets.
<b>attackname</b>	Attack name.
<b>srcport</b>	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.

<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>attackid</b>	The identification number of the attack log message.
<b>sensor</b>	Sensor.
<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.



# 16385

**Message ID:** 016385

**Message Description:** attack signature (icmp)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** signature

**Level/Severity:** alert

Log field	Meaning
type	utm
subtype	ips
eventtype	signature
level	alert
date	The date at which the log was recorded.
time	The time at which the log was recorded.
severity	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
srcip	The source IP.
dstip	The destination IP.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
custom	Custom field.
sessionid	Session ID.
status	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
service	The service where the event or activity occurred.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
count	Number of packets.
attackname	Attack name.
icmpid	The source port of the ICMP message.
icmptype	The type of ICMP message.
icmpcode	The destination port of the ICMP message.
attackid	The identification number of the attack log message.

<b>sensor</b>	Sensor.
<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.

# 16386

**Message ID:** 016386

**Message Description:** attack signature (others)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** signature

**Level/Severity:** alert

Log field	Meaning
type	utm
subtype	ips
eventtype	signature
level	alert
date	The date at which the log was recorded.
time	The time at which the log was recorded.
severity	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
srcip	The source IP.
dstip	The destination IP.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
custom	Custom field.
sessionid	Session ID.
status	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
service	The service where the event or activity occurred.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
count	Number of packets.
attackname	Attack name.
attackid	The identification number of the attack log message.
sensor	Sensor.
ref	URL of the FortiGuard IPS database entry for the attack.
user	User name.

<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.

# 18432

**Message ID:** 018432

**Message Description:** attack anomaly (tcp/udp)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** anomaly

**Level/Severity:** alert

Log field	Meaning
type	utm
subtype	ips
eventtype	anomaly
level	alert
date	The date at which the log was recorded.
time	The time at which the log was recorded.
severity	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
srcip	The source IP.
dstip	The destination IP.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
custom	Custom field.
sessionid	Session ID.
status	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
service	The service where the event or activity occurred.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
count	Number of packets.
attackname	Attack name.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
attackid	The identification number of the attack log message.
sensor	Sensor.

<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.

# 18433

**Message ID:** 018433

**Message Description:** attack anomaly (icmp)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** anomaly

**Level/Severity:** alert

Log field	Meaning
type	utm
subtype	ips
eventtype	anomaly
level	alert
date	The date at which the log was recorded.
time	The time at which the log was recorded.
severity	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
srcip	The source IP.
dstip	The destination IP.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
custom	Custom field.
sessionid	Session ID.
status	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
service	The service where the event or activity occurred.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
count	Number of packets.
attackname	Attack name.
icmpid	The source port of the ICMP message.
icmptype	The type of ICMP message.
icmpcode	The destination port of the ICMP message.
attackid	The identification number of the attack log message.

<b>sensor</b>	Sensor.
<b>ref</b>	URL of the FortiGuard IPS database entry for the attack.
<b>user</b>	User name.
<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.



# 18434

**Message ID:** 018434

**Message Description:** attack anomaly (others)

**Type (type):** utm

**Subtype (subtype):** ips

**Event Type (eventtype):** anomaly

**Level/Severity:** alert

Log field	Meaning
type	utm
subtype	ips
eventtype	anomaly
level	alert
date	The date at which the log was recorded.
time	The time at which the log was recorded.
severity	The priority level of the attack log. Can be <i>info</i> , <i>low</i> , <i>medium</i> , <i>high</i> , or <i>critical</i> .
srcip	The source IP.
dstip	The destination IP.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstintf	The destination interface.
policyid	The ID number of the firewall policy that applies to the session or packet.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
custom	Custom field.
sessionid	Session ID.
status	The status of the packet that was flagged as part of an attack. Can be <i>detected</i> , <i>dropped</i> , or <i>reset</i> .
proto	The protocol number that applies to the session or packet. This is the protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).
service	The service where the event or activity occurred.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
count	Number of packets.
attackname	Attack name.
attackid	The identification number of the attack log message.
sensor	Sensor.
ref	URL of the FortiGuard IPS database entry for the attack.
user	User name.

<b>group</b>	The group name.
<b>srcname</b>	The name of the source device, if it has one. Ex. "MACMINI-#####" , or "My PC".
<b>osname</b>	Name of the device's OS.
<b>osversion</b>	Version number (if available) of the device's OS.
<b>unauthuser</b>	Unauthenticated user name.
<b>unauthusersource</b>	Method used to detect username.
<b>incidentserialno</b>	Incident serial number.

# Spam

## 20480

**Message ID:** 020480

**Message Description:** antispam smtp (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** smtp

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	smtp
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indextid	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthusersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.

<b>dstport</b>	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
<b>dstintf</b>	The destination interface.
<b>service</b>	The service where the event or activity occurred.
<b>profile</b>	The name of the profile that was used to detect and take action.
<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.

# 20481

**Message ID:** 020481

**Message Description:** antispam smtp (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** smtp

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	smtp
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.
<b>subject</b>	Subject.

# 20482

**Message ID:** 020482

**Message Description:** antispam pop3 (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** pop3

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	pop3
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.



# 20483

**Message ID:** 020483

**Message Description:** antispam pop3 (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** pop3

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	pop3
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.

# 20484

**Message ID:** 020484

**Message Description:** antispam imap (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** imap

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	imap
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.

# 20485

**Message ID:** 020485

**Message Description:** antispam endpoint filter (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.

# 20486

**Message ID:** 020486

**Message Description:** antispam endpoint filter (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.



# 20487

**Message ID:** 020487

**Message Description:** antispam endpoint filter (mm7 warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>agent</b>	Agent.

# 20488

**Message ID:** 020488

**Message Description:** antispam endpoint filter (mm7 notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>agent</b>	Agent.

# 20489

**Message ID:** 020489

**Message Description:** antispam endpoint filter (mm1 warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the message. Either <i>tx</i> or <i>rx</i> .
<b>agent</b>	Agent.

# 20490

**Message ID:** 020490

**Message Description:** antispam endpoint filter (mm1 notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** endpointfilter

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	endpointfilter
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the message. Either <i>tx</i> or <i>rx</i> .
<b>agent</b>	Agent.



# 20491

**Message ID:** 020491

**Message Description:** antispam imap banned-word (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** imap

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	imap
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.
<b>subject</b>	Subject.

# 20492

**Message ID:** 020492

**Message Description:** antispam MM1 flood detection (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the message. Either <i>tx</i> or <i>rx</i> .
<b>agent</b>	Agent.

# 20493

**Message ID:** 020493

**Message Description:** antispam MM1 flood detection (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the message. Either <i>tx</i> or <i>rx</i> .
<b>agent</b>	Agent.

# 20494

**Message ID:** 020494

**Message Description:** antispam MM4 flood detection (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.



# 20495

**Message ID:** 020495

**Message Description:** antispam MM4 flood detection (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.

# 20496

**Message ID:** 020496

**Message Description:** antispam MM1 duplicate detection (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the traffic: <i>incoming</i> , <i>outgoing</i> , or <i>N/A</i> .
<b>agent</b>	Agent.

# 20497

**Message ID:** 020497

**Message Description:** antispam MM1 duplicate detection (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>direction</b>	The direction of the traffic: <i>incoming</i> , <i>outgoing</i> , or <i>N/A</i> .
<b>agent</b>	Agent.

# 20498

**Message ID:** 020498

**Message Description:** antispam MM4 duplicate detection (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** warning

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	warning
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.



# 20499

**Message ID:** 020499

**Message Description:** antispam MM4 duplicate detection (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mms

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mms
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.

# 20500

**Message ID:** 020500

**Message Description:** antispam msn hotmail (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** msn

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	msn
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.

# 20501

**Message ID:** 020501

**Message Description:** antispam yahoo mail (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** yahoo

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	yahoo
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.

# 20502

**Message ID:** 020502

**Message Description:** antispam gmail (notice)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** google

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	google
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.



# 20503

**Message ID:** 020503

**Message Description:** antispam smtp general (info)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** smtp

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	smtp
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.

# 20504

**Message ID:** 020504

**Message Description:** antispam pop3 general (info)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** pop3

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	pop3
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.

# 20505

**Message ID:** 020505

**Message Description:** antispam imap general (info)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** imap

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	imap
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.
<b>cc</b>	Alternate destination addresses.
<b>attachment</b>	Email attachment.

# 20506

**Message ID:** 020506

**Message Description:** antispam mapi (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mapi

**Level/Severity:** information

Log field	Meaning
type	utm
subtype	spam
eventtype	mapi
level	information
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.



# 20507

**Message ID:** 020507

**Message Description:** antispam mapi (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mapi

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mapi
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>banword</b>	Banned word flagged in the message.

# 20508

**Message ID:** 020508

**Message Description:** antispam mapi (warning)

**Type (type):** utm

**Subtype (subtype):** spam

**Event Type (eventtype):** mapi

**Level/Severity:** notice

Log field	Meaning
type	utm
subtype	spam
eventtype	mapi
level	notice
date	The date at which the log was recorded.
time	The time at which the log was recorded.
policyid	The ID number of the firewall policy that applies to the session or packet.
custom	Custom field.
indentidx	The identity-based policy identification number. This field displays zero if the firewall policy does not use an identity-based policy; otherwise, it displays the number of the identity-based policy entry that the traffic matched. This number is not globally unique, it is only locally unique within a given firewall policy.
sessionid	Session ID.
user	User name.
group	The group name.
srcname	The name of the source device, if it has one. Ex. "MACMINI-#####", or "My PC".
osname	Name of the device's OS.
osversion	Version number (if available) of the device's OS.
unauthuser	Unauthenticated user name.
unauthersource	Method used to detect username.
vd	The virtual domain in which the logging occurred. If VDOMs are not configured, this will display "root".
srcip	The source IP.
srcport	The source port of the TCP or UDP traffic. The source port appears as zero for other types of traffic.
srcintf	The source interface. For outgoing traffic originating from the firewall, it is <i>unknown</i> .
dstip	The destination IP.
dstport	The destination port number of the TCP or UDP traffic. The destination port appears as zero for other types of traffic.
dstintf	The destination interface.
service	The service where the event or activity occurred.
profile	The name of the profile that was used to detect and take action.

<b>profiletype</b>	The type of profile responsible for the UTM action taken.
<b>status</b>	The status of the email message. One of: <i>exempted</i> , <i>blocked</i> , or <i>detected</i> .
<b>from</b>	Source identifier.
<b>to</b>	Destination identifier.
<b>tracker</b>	Tracker ID.
<b>sentbyte</b>	The number of sent bytes related to the log message.
<b>rcvdbyte</b>	The number of received bytes related to the log message.
<b>subject</b>	Subject.
<b>size</b>	The size of the message/attachments.





























































































































































































































































































































































































































































































































































































































































































































































# Addendum: Variable Event Logs

All logs below are in the category: Event.

These log messages were not documented in the previous versions of the 5.0 Log Message Reference due to their variable structure not fitting the format. They will be documented here instead. This issue is specific to 5.0, and future versions of the LMR will not require an addendum.

The Format column lists the log fields present in that log message. [s] represents a string of text or characters. [n] represents a number or value.

ID	Severity	Subtype	Macro	Format	Description
20001	information	system	LOG_ID_CLIENT_DISASSOCIATED	client [s] is disassociated	paed log
20002	notice	system	LOG_ID_DOMAIN_UNRESOLVABLE	user=system ui=system action=[s] status=failure msg="Can't resolve the IP address of [s]"	The domain name in alert e-mail.s sender is not resolvable
20003	notice	system	LOG_ID_MAIL_SENT_FAIL	user=system ui=system action=alert-email status=failure count=[n] msg="Failed to send alert email from [s] to ([s])"	The alert e-mail send failed
20004	unknown	system	LOG_ID_POLICY_TOO_BIG	user="[s]" ui=[s] status=failure msg="Policy [n] is too big for system, it's installed partially."	Policy is too big
20005	information	system	LOG_ID_PPP_LINK_UP	msg="modem: PPP link is up"	modem log
20006	information	system	LOG_ID_PPP_LINK_DOWN	msg="modem: PPP link is down"	modem log
20007	critical	system	20007	service=kernel status=failure proto=[n] src=[n].[n].[n].[n] src_port=[n] nat=[n].[n].[n].[n] dst=[n].[n].[n].[n] dst_port=[n] msg="NAT port is exhausted."	Socket is exhausted
20011	information	system	LOG_ID_CLIENT_NEW_ASSOCIATION	Accepted association from [s]	paed log
20012	information	system	LOG_ID_CLIENT_WPA_1X	Client [s] does 1X	paed log
20013	information	system	LOG_ID_CLIENT_WPA_SSN	Client [s] does WPA	paed log

ID	Severity	Subtype	Macro	Format	Description
20014	warning	system	LOG_ID_TEST	user="admin" action="login" status="success" msg="user admin logged into the fw - [n]"	test
20015	information	system	LOG_ID_IEEE802_NEW_ STATION	action=authentication status=start msg="Client does 801.1x"	wpad log
20016	information	system	LOG_ID_MODEM_EXCEED_ REDIAL_COUNT	msg="modem: Redial limit exceeded... giving up"	modemd log
20017	information	system	LOG_ID_MODEM_FAIL_TO_ OPEN	msg="modem: unable to open modem device - check hardware"	modemd log
20018	critical	system	LOG_ID_GW_GRP_STATE_ CHANGED	interface="[s]" gw_ group=[n] status=[s] gw_ status=[s] msg="The status of [s] for gateway group [n] is [s]"	Gateway group state is changed
20019	critical	system	LOG_ID_ROUTE_INFO_ CHANGED	interface="[s]" status=[s] msg="[s]"	Routing information is changed because the gateway is up/down
20021	information	system	LOG_ID_MAIL_RESENT	user=system ui=system action=alert-email status=success count=[n] msg="Resending alert e-mail with [n] pending alert(s) from [s] to ([s])"	The alert e-mail resend
20025	notice	system	LOG_ID_REPORTD_ REPORT_SUCCESS	msg="Report generation succeeded for layout:[s]." file="[s]" filesize=[n] datarange="[s]" reporttype="[s]" processtime=[n]	Reporting Complete
20026	error	system	LOG_ID_REPORTD_ REPORT_FAILURE	msg="[s]"	Reporting Failure
20027	warning	system	LOG_ID_REPORT_DEL_OLD_ REC	msg="Delete old report db records" datarange="[s]"	Delete old report db records
20031	critical	system	LOG_ID_RAD_OUT_OF_MEM	msg="Interface [s] Out of memory in [s]:[s]:[n]"	ravdv_iface_set_config() finds a pointer pointing to a wrong address
20032	critical	system	LOG_ID_RAD_NOT_FOUND	msg="Interface [s] not found in [s]:[s]:[n]"	ravdv_iface_same_config() cannot find the corresponding interface by name
20033	information	system	LOG_ID_RAD_MOBILE_IPV6	msg="using Mobile IPv6 extensions"	An interface uses Mobile IPv6 extensions

ID	Severity	Subtype	Macro	Format	Description
20034	critical	system	LOG_ID_RAD_IPV6_OUT_OF_RANGE	msg="MinRtrAdvInterval for [s] must be between [n] and [n]"	MinRtrAdvInterval using Mobile Ipv6 extension is out of range
20035	critical	system	LOG_ID_RAD_MIN_OUT_OF_RANGE	msg="MinRtrAdvInterval must be between [n] and [n] for [s]"	MinRtrAdvInterval is out of range
20036	critical	system	LOG_ID_RAD_MAX_OUT_OF_RANGE	msg="MaxRtrAdvInterval for [s] must be between [n] and [n]"	MaxRtrAdvInterval using Mobile Ipv6 extension is out of range
20037	critical	system	LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE	msg="MaxRtrAdvInterval must be between [n] and [n] for [s]"	MaxRtrAdvInterval is out of range
20038	critical	system	LOG_ID_RAD_MTU_OUT_OF_RANGE	msg="AdvLinkMTU must be zero or between [n] and [n] for [s]"	AdvLinkMTU is out of range
20039	critical	system	LOG_ID_RAD_MTU_TOO_SMALL	msg="AdvLinkMTU must be zero or greater than [n] for [s]"	AdvLinkMTU is too small
20040	critical	system	LOG_ID_RAD_TIME_TOO_SMALL	msg="AdvReachableTime must be less than [n] for [s]"	AdvReachableTime is too small
20041	critical	system	LOG_ID_RAD_HOP_OUT_OF_RANGE	msg="AdvCurHopLimit must not be greater than [n] for [s]"	AdvCurHopLimit in Router Advertisement packet is too big
20042	critical	system	LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE	msg="AdvDefaultLifetime for [s] must be zero or between [n] and [n]"	AdvCurHopLimit in Router Advertisement packet is out of range
20043	critical	system	LOG_ID_RAD_AGENT_OUT_OF_RANGE	msg="HomeAgentLifetime must be between [n] and [n] for [s]"	HomeAgentLifetime in Router Advertisement packet is out of range
20044	critical	system	LOG_ID_RAD_AGENT_FLAG_NOT_SET	msg="AdvHomeAgentFlag must be set with HomeAgentInfo"	AdvHomeAgentFlag HomeAgentLifetime in Router Advertisement packet must be set with HomeAgentInfo
20045	critical	system	LOG_ID_RAD_PREFIX_TOO_LONG	msg="invalid prefix length for [s]"	prefix length is too long
20046	critical	system	LOG_ID_RAD_PREF_TIME_TOO_SMALL	msg="AdvValidLifetime must be greater than AdvPreferredLifetime for [s]"	AdvValidLifetime is less than AdvPreferredLifetime
20047	critical	system	LOG_ID_RAD_FAIL_IPV6_SOCKET	msg="can't create socket(AF_INET6): [s]"	IPv6 router advertisement daemon (radvd) failed to create an IPv6 socket
20048	critical	system	LOG_ID_RAD_FAIL_OPT_IPV6_PKTINFO	msg="setsockopt(IPV6_PKTINFO): [s]"	Radvd failed to set IPV6_PKTINFO option

ID	Severity	Subtype	Macro	Format	Description
20049	critical	system	LOG_ID_RAD_FAIL_OPT_IPV6_CHECKSUM	msg="setsockopt(IPV6_CHECKSUM): [s]"	Radvd failed to set IPV6_CHECKSUM option
20050	critical	system	LOG_ID_RAD_FAIL_OPT_IPV6_UNICAST_HOPS	msg="setsockopt(IPV6_UNICAST_HOPS): [s]"	Radvd failed to set IPV6_UNICAST_HOPS option
20051	critical	system	LOG_ID_RAD_FAIL_OPT_IPV6_MULTICAST_HOPS	msg="setsockopt(IPV6_MULTICAST_HOPS): [s]"	Radvd failed to set IPV6_MULTICAST_HOPS option
20052	critical	system	LOG_ID_RAD_FAIL_OPT_IPV6_HOPLIMIT	msg="setsockopt(IPV6_HOPLIMIT): [s]"	Radvd failed to set IPV6_HOPLIMIT option
20053	critical	system	LOG_ID_RAD_FAIL_OPT_IPPROTO_ICMPV6	msg="setsockopt(ICMPV6_FILTER): [s]"	Radvd failed to set ICMPV6_FILTER option
20054	information	system	LOG_ID_RAD_EXIT_BY_SIGNAL	msg="radvd receive signal=[n]"	radvd has received a signal, and is going to exit
20055	critical	system	LOG_ID_RAD_FAIL_CMDB_QUERY	msg="Can not create query to interface at [s]:[s]:[n]!"	Radvd cannot create query to interface by using cmf_query_create()
20056	critical	system	LOG_ID_RAD_FAIL_CMDB_FOR_EACH	msg="Internal error in cmf_query_for_each()!"	Radvd occurs an internal error when it uses cmf_query_for_each()
20057	critical	system	LOG_ID_RAD_FAIL_FIND_VIRT_INTF	msg="Interface [s]:[n] not found in the list!"	Radvd failed to find a virtual interface by interface index
20058	information	system	LOG_ID_RAD_UNLOAD_INTF	msg="Interface [s]:[n] unloaded!"	Radvd reloads a specific interface
20059	warning	system	LOG_ID_RAD_NO_PKT_INFO	msg="received packet with no pkt_info!"	Radvd received a packet with no pkt_info
20060	warning	system	LOG_ID_RAD_INV_ICMPV6_LEN	msg="received icmpv6 packet with invalid length: [n]"	Radvd received an icmpv6 packet with invalid length
20061	critical	system	LOG_ID_RAD_INV_ICMPV6_TYPE	msg="icmpv6 filter failed"	Radvd received an unwanted type of icmpv6 packet
20062	warning	system	LOG_ID_RAD_INV_ICMPV6_RA_LEN	msg="received icmpv6 RA packet with invalid length: [n]"	Radvd received icmpv6 RA packet with invalid length
20063	warning	system	LOG_ID_RAD_ICMPV6_NO_SRC_ADDR	msg="received icmpv6 RA packet with non-linklocal source address"	Radvd received icmpv6 RA packet with non-linklocal source address
20064	warning	system	LOG_ID_RAD_INV_ICMPV6_RS_LEN	msg="received icmpv6 RS packet with invalid length: [n]"	Radvd received icmpv6 RS packet with invalid length
20065	warning	system	LOG_ID_RAD_INV_ICMPV6_CODE	msg="received icmpv6 RS/RA packet with invalid code: [n]"	Radvd received icmpv6 RS/RA packet with invalid code

ID	Severity	Subtype	Macro	Format	Description
20066	warning	system	LOG_ID_RAD_INV_ICMPV6_HOP	msg="received RS or RA with invalid hoplimit [n] from [s]"	Radvd received icmpv6 RS/RA packet with wrong hoplimit
20067	warning	system	LOG_ID_RAD_MISMATCH_HOP	msg="our AdvCurHopLimit on [s] doesn't agree with [s]"	AdvCurHopLimit on our interface does not agree with a remote site
20068	warning	system	LOG_ID_RAD_MISMATCH_MGR_FLAG	msg="our AdvManagedFlag on [s] doesn't agree with [s]"	AdvManagedFlag on our interface does not agree with a remote site
20069	warning	system	LOG_ID_RAD_MISMATCH_OTH_FLAG	msg="our AdvOtherConfigFlag on [s] doesn't agree with [s]"	AdvOtherConfigFlag on our interface does not agree with a remote site
20070	warning	system	LOG_ID_RAD_MISMATCH_TIME	msg="our AdvReachableTime on [s] doesn't agree with [s]"	AdvReachableTime on our interface does not agree with a remote site
20071	warning	system	LOG_ID_RAD_MISMATCH_TIMER	msg="our AdvRetransTimer on [s] doesn't agree with [s]"	AdvRetransTimer on our interface does not agree with a remote site
20072	critical	system	LOG_ID_RAD_EXTRA_DATA	msg="trailing garbage in RA on [s] from [s]"	Radvd finds extra data in RA packet
20073	critical	system	LOG_ID_RAD_NO_OPT_DATA	msg="zero length option in RA on [s] from [s]"	Radvd finds a RA packet with no option data
20074	critical	system	LOG_ID_RAD_INV_OPT_LEN	msg="option length greater than total length in RA on [s] from [s]"	option length is greater than total length in RA packet
20075	warning	system	LOG_ID_RAD_MISMATCH_MTU	msg="our AdvLinkMTU on [s] doesn't agree with [s]"	AdvLinkMTU on our interface does not agree with a remote site
20077	warning	system	LOG_ID_RAD_MISMATCH_PREF_TIME	msg="our AdvPreferredLifetime on [s] for [s] doesn't agree with [s]"	AdvPreferredLifetime on our interface does not agree with a remote site
20078	critical	system	LOG_ID_RAD_INV_OPT	msg="invalid option [n] in RA on [s] from [s]"	Radvd finds an invalid option in RA packet from a remote site
20079	information	system	LOG_ID_RAD_READY	msg="radvd started"	Radvd daemon is ready to serve
20080	critical	system	LOG_ID_RAD_FAIL_TO_RCV	msg="recvmsg: [s]"	Recvmsg() in radvd failed
20081	critical	system	LOG_ID_RAD_INV_HOP	msg="received a bogus IPV6_HOPLIMIT from the kernel! len=[n], data=[n]"	Radvd received a packet with a wrong IPV6_HOPLIMIT
20082	critical	system	LOG_ID_RAD_INV_PKTINFO	msg="received a bogus IPV6_PKTINFO from the kernel! len=[n], index=[n]"	Radvd received a packet with a wrong IPV6_PKTINFO

ID	Severity	Subtype	Macro	Format	Description
20083	warning	system	LOG_ID_RAD_FAIL_TO_CHECK	msg="problem checking all-routers membership on [s]"	Radvd failed to check whether we've joined the all-routers multicast group
20084	warning	system	LOG_ID_RAD_FAIL_TO_SEND	msg="sendmsg: [s]"	sendmsg () in radvd failed
20085	information	system	20085	status="clash" proto=[n] msg="session clash"[s]	session clash
20086	unknown	system	20086	msg="==[s] xh0(sp_[n], fmc[n]) crashed, master is fmc[n]=="	xh0 crashed
20090	notice   information	system	LOG_ID_INTF_LINK_STA_CHG	intf=[s] status=[s] msg="interface [s] link status is [s]"	Interface link status changed
20101	warning	system	LOG_ID_WEB_LIC_EXPIRE	msg="FortiGuard web filtering license will expire in [n] day(s)"	FortiGuard web filtering license expiring
20102	warning	system	LOG_ID_SPAM_LIC_EXPIRE	msg="FortiGuard anti-spam license will expire in [n] day(s)"	FortiGuard anti-spam license expiring
20103	warning	system	LOG_ID_AV_LIC_EXPIRE	msg="FortiGuard AV update license will expire in [n] day(s)"	FortiGuard AV update license expiring
20104	warning	system	LOG_ID_IPS_LIC_EXPIRE	msg="FortiGuard IPS update license will expire in [n] day(s)"	FortiGuard IPS update license expiring
20105	warning	system	LOG_ID_LOG_UPLOAD_SKIP	ui=[s] action=upload error="Daily volume exceeded" msg="Log upload to FortiCloud skipped (Daily volume exceeded)."	Log uploading
20107	warning	system	LOG_ID_LOG_UPLOAD_ERR	action=upload error="[s]" user="[s]" server=[s] port=[n] msg="Log upload to [s] error on vdom [s]"	uploading error
20108	notice	system	LOG_ID_LOG_UPLOAD_DONE	action=upload status=completed user="[s]" server=[s] port=[n] msg="Log upload to [s] completed on vdom [s]"	upload status
20110	notice	system	LOG_ID_HPAPI_ESPD_START	msg="hp_api: Connection to ESPd has been initialized"	hp_api log
20111	warning	system	LOG_ID_HPAPI_ESPD_RESET	msg="hp_api: Connection to ESPd has been reset, exiting"	hp_api log

ID	Severity	Subtype	Macro	Format	Description
20113	error	system	LOG_ID_IPSA_DOWNLOAD_FAIL	msg="Fail to download IPSA DB!"	IPSA error
20114	error	system	LOG_ID_IPSA_SELFTEST_FAIL	msg="IPSA self test failed, disable IPSA!"	IPSA error
20115	error	system	LOG_ID_IPSA_STATUSUPD_FAIL	msg="Fail to update IPSA driver status!"	IPSA error
20200	notice	system	LOG_ID_FIPS_SELF_TEST	user="[s]" ui=[s] action=self-test msg="Administrator [s] initiates the [s] self-test from [s]"	running self-test
20201	notice	system	LOG_ID_FIPS_SELF_ALL_TEST	user="[s]" ui=[s] action=self-test msg="Administrator [s] initiates all self-tests from [s]"	running self-test
20202	warning	system	LOG_ID_DISK_FORMAT_ERROR	msg="Partitioning or formatting error ([s], [s]) partition=[n] format=[n] label=[s]"	Error in partitioning or formatting
20203	information	system	LOG_ID_DAEMON_SHUTDOWN	action=daemon-shutdown daemon=[s] pid=[n] msg="[s] shut down"	daemon shutdown
20204	information	system	LOG_ID_DAEMON_START	action=daemon-startup daemon=[s] pid=[n] msg="[s] has started"	daemon started
20205	critical	system	LOG_ID_DISK_FORMAT_REQ	user="[s]" ui=[s] action=format-disk msg="User [s] requested to format [s] disk from [s]"	format disk
20206	warning	system	LOG_ID_DISK_SCAN_REQ	user="[s]" ui=[s] action=scan-disk msg="User [s] requested to scan [s] disk from [s]"	scan disk
20300	unknown	system	LOG_ID_BGP_NB_STAT_CHG	msg="BGP: %%BGP-5-ADJCHANGE: neighbor [s] [s] [s]"	bgp neighbor status change
22000	warning	system	LOG_ID_INV_PKT_LEN	msg="Packet length does not match that specified in the request header."	Packet length does not match that specified in the request header.
22001	warning	system	LOG_ID_UNSUPPORTED_PROT_VER	msg="Protocol version-[n] is not supported"	Unsupported protocol version
22002	warning	system	LOG_ID_INV_REQ_TYPE	msg="Request type [n] is not supported."	Other request than http, https, ftp, mail and av is not supported



ID	Severity	Subtype	Macro	Format	Description
22003	warning	system	LOG_ID_FAIL_SET_SIG_HANDLER	sigaction([n])failed: [s]	failed to set up a signal handler
22004	warning	system	LOG_ID_FAIL_CREATE_SOCKET	Socket() failed: [s]	failed to create a socket
22005	warning	system	LOG_ID_FAIL_CREATE_SOCKET_RETRY	failed to create a [s]/udp socket to receive URL request: [s]	failed to create a udp socket to receive URL request
22006	warning	system	LOG_ID_FAIL_REG_CMDB_EVENT	msg="Failed to register for cmdb events."	Failed to register for cmdb events
22009	warning	system	LOG_ID_FAIL_FIND_AV_PROFILE	name=[s] status=failure msg="failed to find its AV protection profile"	failed to find av profile by ID
22010	error	system	LOG_ID_SENDDTO_FAIL	process="[s]" reason="[s]" msg="failed to send urfilter packet"	safe_sendto() failed
22011	unknown	system	22011	service=kernel conserve=on free="[n] pages" red="[n] pages" msg="Kernel enters conserve mode"	Kernel enters conserve mode
22012	unknown	system	22012	service=kernel conserve=exit free="[n] pages" green="[n] pages" msg="Kernel leaves conserve mode"	Kernel leaves conserve mode
22013	alert	system	22013	action=pba-block-exhaust saddr=[n].[n].[n].[n] poolname="[s]" msg="Pba ippool port-block has been exhausted"	Alert ippool pba block exhaust
22014	alert   notice	system	22014	action=pba-natip-exhaust saddr=[n].[n].[n].[n] poolname="[s]" msg="Pba ippool natip has been exhausted"	Alert ippool pba natip exhaust
22015	notice	system	LOG_ID_EXCEED_VD_RES_LIMIT	service=kernel msg="[s] vdom([n]) limit. count=[n] limit=[n]"	Exceed vdom resource limit
22016	notice	system	22016	action=pba-close saddr=[n].[n].[n].[n] nat=[n].[n].[n].[n] portbegin=[n] portend=[n] poolname="[s]" duration=[n] msg="Pba ippool close"	Deallocate ippool pba
22020	warning	system	LOG_ID_FAIL_CREATE_HA_SOCKET	msg="Socket() failed: [s]"	Failed to create a ha_socket

ID	Severity	Subtype	Macro	Format	Description
22021	warning	system	LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY	msg="Failed to create a udp socket to relay URL requests: [s]"	Failed to create a udp socket to relay URL requests
22100	warning	system	LOG_ID_QUAR_DROP_TRAN_JOB	count=[n] duration=[n] limit=[n] used=[n] fams_pause=[n] action=transfer status=drop reason=[s] msg="In the past [n] seconds, [n] files were dropped by quard."	Quarantine dropped transfer jobs
22101	warning	system	LOG_ID_QUAR_DROP_TLL_JOB	count=[n] action=transfer status=drop reason=poor-network-condition msg="[n] files were dropped by quard to [s]: [n] reached max retries, [n] reached TTL."	Quarantine dropped transfer jobs
22102	critical	system	LOG_ID_LOG_DISK_FAILURE	msg="Log disk failure is imminent, logs should be backed up"	Erroneous SMART status
22104	critical	system	22104	action=power-supply-monit or status=restore unit=[s] msg="Power supply [s] restore"	Power supply restore
22105	critical	system	LOG_ID_POWER_FAILURE	action=power-supply-monit or status=failure unit=[s] msg="Power supply [s] [s]"	Power supply failure
22106	warning   information	system	LOG_ID_POWER_OPTIONAL_NOT_DETECTED	action=ipmc-sensor-monitor status=failure msg="[s]"	IPMC sensor failure
22107	warning	system	LOG_ID_VOLT_ANOM	action=ipmc-sensor-monitor status=failure msg="[s]"	IPMC sensor failure
22108	warning	system	LOG_ID_FAN_ANOM	action=ipmc-sensor-monitor status=failure msg="[s]"	IPMC sensor failure
22110	critical	system	LOG_ID_SPARE_BLOCK_LOW	msg="Available spare blocks of boot device are getting low (remaining [n])."	Available spare blocks is low
22200	warning	system	LOG_ID_AUTO_UPT_CERT	user=system action=certificate-update status=warning cert=[s] msg="CA certificate [s] will auto-update in [n] days."	Certificate will be auto-update
22201	warning	system	LOG_ID_AUTO_GEN_CERT	user=system action=certificate-regenerate status=warning cert=[s] msg="Local certificate [s] will auto-regenerate in [n] days."	Certificate will be auto-regenerate

ID	Severity	Subtype	Macro	Format	Description
22202	error	system	LOG_ID_AUTO_UPT_CERT_FAIL	user=system action=certificate-update status=failure cert=[s] msg="[s]"	Certificate failed to auto-update
22203	error	system	LOG_ID_AUTO_GEN_CERT_FAIL	user=system action=certificate-regenerate status=failure cert=[s] msg="[s]"	Certificate failed to auto-regenerate
22700	critical	system	LOG_ID_IPS_FAIL_OPEN	msg="IPS session scan resumed, exit fail open mode."	IPS fail open
22800	critical	system	LOG_ID_SCAN_SERV_FAIL	service=[s] mode=[s] msg="The system has [s] session fail mode"	Scan services session fail mode
22801	critical	system	LOG_ID_SCAN_LEAVE_CONSERVE_MODE	service=[s] conserve=exit total=[n] free=[n] entermargin=[n] exitmargin=[n] msg="The system exited conserve mode"	Scan services exited conserve mode
22802	critical	system	LOG_ID_SYS_ENTER_CONSERVE_MODE	service=[s] sysconserve=on total=[n] free=[n] entermargin=[n] exitmargin=[n] msg="The system has entered system conserve mode"	System services entered conserve mode
22803	critical	system	LOG_ID_SYS_LEAVE_CONSERVE_MODE	service=[s] sysconserve=exit total=[n] free=[n] entermargin=[n] exitmargin=[n] msg="The system exited system conserve mode"	System exited conserve mode
22804	critical	system	LOG_ID_LIC_STATUS_CHG	service=license status=[s] msg="License status changed to [s]"	License Status Change
22805	warning	system	LOG_ID_FAIL_TO_VALIDATE_LIC	service=license status=warning msg="License could not be validated for over 4 hours"	License Status Warning
22806	warning	system	LOG_ID_DUP_LIC	service=license status=warning msg="Detected duplicate license in use"	License Status Duplicate Warning
22810	critical	system	LOG_ID_SCAN_ENTER_CONSERVE_MODE	service=[s] conserve=on total=[n] free=[n] entermargin=[n] exitmargin=[n] msg="The system has entered conserve mode"	Scan services entered conserve mode

ID	Severity	Subtype	Macro	Format	Description
22900	notice	system	LOG_ID_CAPUTP_SESSION	msg="[s]" action=[s] src=[n].[n].[n].[n]	caputp-session
22901	notice	system	LOG_ID_FAZ_CON	action=connect status=success msg="Connected to FortiAnalyzer [s]"	FortiAnalyzer Connection
22902	notice	system	LOG_ID_FAZ_DISCON	action=disconnect status=success reason="[s]" msg="Disconnected from FortiAnalyzer [s]"	FortiAnalyzer Disconnection
22903	critical	system	LOG_ID_FAZ_CON_ERR	action=connect status=failure reason="[s]" msg="Failed to connect FortiAnalyzer [s]"	FortiAnalyzer Connection
22910	notice	system	LOG_ID_EVENT_SLA_PROBE_PING	[s]="[n]" [s]="[s]" [s]="ping" [s]="[s]" msg="SLA Probe event: change state from [s] to [s]"	SLA Probe information
22911	notice	system	LOG_ID_EVENT_SLA_PROBE_HTTPGET	[s]="[n]" [s]="[s]" [s]="[s]" [s]="http-get" [s]="[s]" msg="SLA Probe event: change state from [s] to [s]"	SLA Probe information
22916	notice	system	LOG_ID_FDS_STATUS	status=[s] msg="FortiGuard Message Service server is [s]"	FortiGuard Message Service status
22917	notice	system	LOG_ID_FDS_SMS_QUOTA	user=system msg="SMS quota is used up."	SMS quota used up
23101	unknown	vpn	LOG_ID_IPSEC_TUNNEL_UP	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
23102	unknown	vpn	LOG_ID_IPSEC_TUNNEL_DOWN	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
23103	unknown	vpn	LOG_ID_IPSEC_TUNNEL_STAT	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
26001	information   unknown	router	LOG_ID_DHCP_MSG	interface="[s]" dhcp_ msg="[s]" dir=[s] mac=[s]:[s]:[s]:[s]:[s]:[s] ip=[n].[n].[n].[n] lease=[n] hostname="[s]" msg="[s]"	DHCP request and response log

ID	Severity	Subtype	Macro	Format	Description
26002	error	router	LOG_ID_DHCP_NO_SHARE_NET	interface="[s]" No shared network for network [s] ([s])	No shared network found
26003	information	router	LOG_ID_DHCP_STAT	interface="[s]" total=[n] used=[n] msg="[s]"	DHCP Statistics
26004	error	router	LOG_ID_DHCP_MULT_SUB_NET	interface="[s]" Address range [s] to [s], netmask [s] spans [s]!	Address range spans multiple subnets
26005	error	router	LOG_ID_DHCP_INV_ADDR_RANGE	interface="[s]" Address range [s] to [s] not on net [s]/[s]!	Address range doesn't belong to the net
29001	unknown	router	LOG_ID_PPPD_MSG	user="[s]" local=[n].[n].[n].[n] remote=[n].[n].[n].[n] assigned=[n].[n].[n].[n] stat="[s]" msg="[s]"	Pppd log message
29002	notice   debug	router	LOG_ID_PPPD_AUTH_SUC	user="[s]" local=[n].[n].[n].[n] remote=[n].[n].[n].[n] assigned=[n].[n].[n].[n] action=auth_success msg="User '[s]' using [s] with authentication protocol [s], [s]"	PPPD authentication success log message
29003	notice	router	LOG_ID_PPPD_AUTH_FAIL	local=[n].[n].[n].[n] remote=[n].[n].[n].[n] assigned=[n].[n].[n].[n] action=auth_failed msg="[s] is trying to connect using [s] with authentication protocol [s], failed"	PPPD authentication failure log message
29009	notice	router	LOG_ID_PPPOE_STATUS_REPORT	gateway=[n].[n].[n].[n] assigned=[n].[n].[n].[n] msg="PPPoE status report"	PPPoE status report
29011	error	router	LOG_ID_PPPD_FAIL_TO_EXEC	Can't execute [s]: [s]	pppd cannot execute a program
29012	unknown	router	LOG_ID_PPP_OPT_ERR	[s]	ppp has received wrong options
29013	notice	router	LOG_ID_PPPD_START	msg="pppd is started"	pppd is started
29014	information	router	LOG_ID_PPPD_EXIT	msg="pppd is exiting"	pppd is exiting
29015	error	router	LOG_ID_PPP_RCV_BAD_PEER_IP	Peer IP is the same as an interface IP[s]. IP([n].[n].[n].[n])	ppp has received bad options
29016	error	router	LOG_ID_PPP_RCV_BAD_LOCAL_IP	Local IP is the same as an interface IP[s]. IP([n].[n].[n].[n])	ppp has received bad options

ID	Severity	Subtype	Macro	Format	Description
29017	unknown	router	LOG_ID_PPP_OPT_NOTIF	[s]	ppp has received wrong options
29020	notice	router	LOG_ID_WIRELESS_SET_FAIL		wireless set command [s] [s] failed
32001	information	system	LOG_ID_ADMIN_LOGIN_SUCC	user="[s]" ui=[s] action=login status=success reason=none profile="[s]" msg="Administrator [s] logged in successfully from [s]"	Admin logged in successfully
32002	alert	system	LOG_ID_ADMIN_LOGIN_FAIL	user=test ui=cli action=login status=failed reason=test msg="Alarm testing"	Failed admin login attempt
32003	information	system	LOG_ID_ADMIN_LOGOUT	user="[s]" ui=[s] action=logout status=success duration=[n] [s]reason=[s] msg="Administrator [s] [s] [s]"	Admin logged out
32004	emergency	system	LOG_ID_ALARM_TEST_FAIL	action=error-mode reason=self-test msg="Alarm testing"	alarm testing
32005	information	system	32005	user="[s]" action=vdom-override status=success reason=none msg="Administrator [s] vdom overridden to [s]"	Admin overrided vdom successfully
32006	information	system	LOG_ID_ADMIN_ENTER_VDOM	user="[s]" ui=[s] action=vdom-switch reason=none msg="User [s] has entered the virtual domain [s]"	A super admin has entered to this vdom
32007	information	system	LOG_ID_ADMIN_LEFT_VDOM	user="[s]" ui=[s] action=vdom-switch reason=none msg="User [s] has left the virtual domain [s]"	A super admin has left the current vdom
32008	warning	system	LOG_ID_VIEW_LOG_FAIL	user="[s]" ui=[s] msg="User [s] [s] failed to access the [s] logs from [s]"	Failed to view log
32009	information	system	LOG_ID_SYSTEM_START	msg="Fortigate started[s]"	System started
32010	emergency   information   unknown	system	LOG_ID_DISK_LOG_FULL	msg="[s] is [n]% full.System will stop [s] logging."	Log full

ID	Severity	Subtype	Macro	Format	Description
32011	notice	system	LOG_ID_LOG_ROLL	action=roll-log reason=file-size log=[s] msg="Disk log has rolled."	Log rotation
32012	information	system	LOG_ID_FIPS_LEAVE_ERR_MOD	action=exit-error-mode msg="System exiting out of error mode."	CC exiting error mode
32014	warning	system	LOG_ID_CS_LIC_EXPIRE	msg="FortiGuard customer support license will expire in [n] day(s)"	FortiGuard customer support license expiring
32015	warning	system	LOG_ID_DISK_LOG_USAGE	msg="Log disk is [n]% full"	Log full
32018	emergency	system	LOG_ID_FIPS_ENTER_ERR_MOD	action=error-mode reason=[s] msg="System enters error-mode due to [s]"	FIPS error mode
32020	warning	system	LOG_ID_SSH_CORRPUT_MAC	ui=https msg="Corrupted MAC packet detected"	Corrupted MAC detected
32021	alert	system	LOG_ID_ADMIN_LOGIN_DISABLE	ui=[s] action=login status=failed reason=exceed_limit msg="Login disabled from IP [s] for [n] seconds because of [n] bad attempts"	Admin login disabled
32022	notice	system	LOG_ID_VDOM_ENABLED	user="[s]" ui=[s] msg="User [s] enabled virtual domain [s] from [s]"	vdom enabled
32023	warning   information	system	LOG_ID_MEM_LOG_FULL	msg="Memory log is [n]% full"	Log full
32024	notice	system	LOG_ID_ADMIN_PASSWD_EXPIRE	user="[s]" action=admin-password status=expired msg="Password of administrator [s] has expired."	Admin password expiry
32026	critical	system	LOG_ID_STORE_CONF_FAIL	Cannot store config due to first line error: require first line in file [s] from process [n]	Cannot store config due to first line error
32027	notice	system	LOG_ID_VIEW_LOG_SUCC	user="[s]" ui=[s] log=[s] msg="User [s] has viewed the disk logs from [s]"	User displayed disk logs
32028	information	system	LOG_ID_LOG_DEL_DIR	msg="System deleted directory [s]."	Log full
32029	information	system	LOG_ID_LOG_DEL_FILE	action=delete msg="System deleted log file [s]"	Log deleted

ID	Severity	Subtype	Macro	Format	Description
32030	notice	system	LOG_ID_SEND_FDS_STAT	user="[s]" ui=[s] action=send-fds-stats msg="User [s] requested to send FDS statistics from [s]"	send fds stats
32035	notice	system	LOG_ID_VDOM_DISABLED	user="[s]" ui=[s] msg="User [s] disabled virtual domain [s] from [s]"	vdom disabled
32045	warning	system	LOG_ID_MGR_LIC_EXPIRE	msg="FortiGuard management service license will expire in [n] day(s)"	FortiGuard management service license expiring
32048	warning	system	LOG_ID_SCHEDULE_EXPIRE	msg="onetime schedule [s] will expire in [n] day(s)"	onetime schedule expiring
32051	notice	system	LOG_ID_LOG_UPLOAD	ui=[s] action=upload status=start msg="Start uploading disk logs to [s] from vdom [s]."	Log uploading
32086	warning	system	LOG_ID_ENTER_TRANSPARENT	user=[s] ui=lcd action=[s] status=success msg="System has been changed to transparent mode LCD via LCD"	System has been changed to transparent mode LCD via LCD
32087	warning	system	LOG_ID_ENTER_NAT	user=[s] ui=lcd action=[s] status=success msg="System has been changed to NAT mode LCD via LCD"	System has been changed to NAT mode LCD via LCD
32095	warning	system	LOG_ID_GUI_CHG_SUB_MODULE	user="[s]" ui=[s] action=[s] status=[s] msg="[s] by user [s] via [s]"	A user has performed an action to the firewall via GUI. The action can be one of the followings: reboot, shutdown, reload, backup, factory_reset, restore, upgrade, switch_mode, download, upload, clear_mlog, del_log, update, downgrade, del_session, bootup
32096	warning	system	LOG_ID_GUI_DOWNLOAD_LOG	user="[s]" ui=[s] action=[s] status=[s] hash=[s] file=[s] msg="[s] by user [s] via [s]"	A user has downloaded a logging file from the firewall via GUI
32100	warning	system	LOG_ID_FORTI_TOKEN_SYNC	user="[s]" action=token_ sync msg="User [s] synchronized his/her FortiToken"	FortiToken synchronization
32101	notice	system	LOG_ID_LCD_CHG_CONF	user="[s]" ui=[s] msg="[s] by [s]"	Administrator has changed configuration from LCD



ID	Severity	Subtype	Macro	Format	Description
32102	unknown	system	LOG_ID_CHG_CONFIG	user="[s]" ui="[s]" module="[s]" submodule="[s]" msg="[s]" made a change from [s]:[s]"	A user has changed the configuration
32103	notice	system	LOG_ID_NEW_FIRMWARE	user=system action=firmware status=new msg="New firmware is available from FortiGuard"	New firmware is available from FortiGuard
32120	notice	system	LOG_ID_RPT_ADD_DATASET	user="[s]" ui="[s]" name="[s]" msg="User [s] added a report dataset [s] from [s]"	Report Dataset is added
32122	notice	system	LOG_ID_RPT_DEL_DATASET	user="[s]" ui="[s]" name="[s]" msg="User [s] delete a report dataset [s] from [s]"	A report dataset is deleted
32123	notice	system	LOG_ID_RPT_ADD_LAYOUT_ITEM	user="[s]" ui="[s]" name="[n]" msg="User [s] added a report summary entry [n] from [s]"	Report Summary entries is added
32124	notice	system	LOG_ID_RPT_DEL_LAYOUT_ITEM	user="[s]" ui="[s]" name="[n]" msg="User [s] delete a report summary entry [n] from [s]"	A report summary entries is deleted
32125	notice	system	LOG_ID_RPT_ADD_CHART	user="[s]" ui="[s]" name="[s]" msg="User [s] added a report chart widget [s] from [s]"	Report Chart widget is added
32126	notice	system	LOG_ID_RPT_DEL_CHART	user="[s]" ui="[s]" name="[s]" msg="User [s] delete a report chart widget [s] from [s]"	A report chart widget is deleted
32129	notice	system	LOG_ID_ADD_GUEST	user="[s]" ui="[s]" name="[s]" status=[s] msg="User [s] added guest user [s] from [s]"	A new guest user is added
32130	notice	system	LOG_ID_CHG_USER	user="[s]" ui="[s]" name="[s]" old_status=[s] new_ status=[s] passwd=[s] msg="User [s] changed local user [s] setting from [s]"	A local user's setting is changed
32131	notice	system	LOG_ID_DEL_GUEST	user="[s]" ui="[s]" name="[s]" status=[s] msg="User [s] deleted guest user [s] from [s]"	A guest user is deleted
32132	notice	system	LOG_ID_ADD_USER	user="[s]" ui="[s]" name="[s]" status=[s] msg="User [s] added local user [s] from [s]"	A new local user is added

ID	Severity	Subtype	Macro	Format	Description
32138	critical	system	LOG_ID_REBOOT		device is rebooted
32139	critical   warning   notice	system	LOG_ID_UPD_SIGN_DB	user="[s]" ui=[s] action=update msg="User [s] requested a geoip object update from [s]"	Update src-vis object.
32140	notice	system	32140	user="[s]" ui=[s] field=date-time msg="The [s] ntp server, [s]([s]), is determined [s] at [s]"	ntp server status change
32142	alert   error   warning   notice	system	LOG_ID_BACKUP_CONF	action=backup status=success msg="Configuration backed up to flash disk after system upgrading"	backup configuration
32143	critical	system	32143	user="[s]" ui="[s]" action=update-image msg="User [s] loaded a wrong layout image from [s]."	update image
32148	notice	system	LOG_ID_GET_CRL	user="[s]" ui=[s] action=crl-update crl=[s] msg="User [s] requested a CRL update from [s]"	get CRL
32149	notice	system	LOG_ID_COMMAND_FAIL	user="[s]" ui=[s] ret=[n] msg="Command failed:'[s]' Return code [n]: [s]"	command failure
32151	notice	system	LOG_ID_ADD_IP6_LOCAL_POL	[s]	A new ipv6 firewall local in policy is added
32152	notice	system	LOG_ID_CHG_IP6_LOCAL_POL	[s]	A ipv6 firewall local in policy's setting is changed
32153	notice	system	LOG_ID_DEL_IP6_LOCAL_POL	[s]	A ipv6 firewall local in policy is deleted
32155	notice	system	LOG_ID_ACT_FTOKEN_REQ	user="[s]" ui=[s] action=fortitoken-activate serialno=[s] msg="User [s] has requested to activate FortiToken [s]."	Activate FortiToken
32156	notice	system	LOG_ID_ACT_FTOKEN_SUCC	action=fortitoken-activate serialno=[s] status=success msg="Activation of FortiToken [s] succeeded."	Activate FortiToken
32157	notice	system	LOG_ID_SYNC_FTOKEN_SUCC	user="[s]" ui=[s] action=fortitoken-synchronize serialno=[s] status=success msg="Administrator [s] resynchronized FortiToken [s] successfully."	Synchronize FortiToken

ID	Severity	Subtype	Macro	Format	Description
32158	notice	system	LOG_ID_SYNC_FTOKEN_FAIL	user="[s]" ui=[s] action=fortitoken-synchronize serialno=[s] status=failed msg="Administrator [s] failed to resynchronize FortiToken [s], because [s]."	Synchronize FortiToken
32159	notice	system	LOG_ID_ACT_FTOKEN_FAIL	action=fortitoken-activate serialno=[s] status=failed msg="Activation of FortiToken [s] failed, because [s]."	Activate FortiToken
32168	notice	system	LOG_ID_REACH_VDOM_LIMIT	user="[s]" ui=[s] msg="Adding new entry failed: vdom property limit has been reached when user [s] adds [s].[s] from [s]"	adding new entry failed
32170	alert	system	LOG_ID_ALARM_MSG	action=alarm alarmid=[n] groupid=[n] msg="[s]"	alarm
32171	alert	system	LOG_ID_ALARM_ACK	user="[s]" ui=[s] action=alarm-ack alarmid=[n] acktime="[s]" msg="[s]"	alarm ack
32172	notice	system	LOG_ID_ADD_IP4_LOCAL_POL	[s]	A new firewall local in policy is added
32173	notice	system	LOG_ID_CHG_IP4_LOCAL_POL	[s]	A firewall local in policy's setting is changed
32174	notice	system	LOG_ID_DEL_IP4_LOCAL_POL	[s]	A firewall local in policy is deleted
32188	warning	system	LOG_ID_SSL_PROXY_CA_INIT_FAIL	msg="SSL Proxy CA initialization failed"	[s]
32200	critical	system	LOG_ID_SHUTDOWN	user="[s]" ui=[s] action=shutdown msg="User [s] shutdown the device from [s].[s]"	shutdown device
32201	critical	system	LOG_ID_LOAD_IMG_SUCC	user="[s]" ui=[s] action=loaded-image msg="User [s] loaded the image from [s], the new image does not support CC mode."	loaded an image
32202	critical	system	LOG_ID_RESTORE_IMG	user="[s]" ui=[s] action=restore-image msg="User [s] restored the image from [s] ([s],build[s] -> [s],build[s])"	restore the image

ID	Severity	Subtype	Macro	Format	Description
32203	critical   warning   notice	system	LOG_ID_RESTORE_CONF	user="[s]" ui="[s]" action=restore-configuration msg="User [s] restored the configuration from [s]"	restore the configuration
32204	critical   notice	system	LOG_ID_RESTORE_FGD_SVR	user="[s]" ui="[s]" action="[s]" msg="User [s] restored [s] file from [s]"	restore the fortiguard service
32205	critical   notice	system	LOG_ID_RESTORE_VDOM_LIC	user="[s]" ui="[s]" action="[s]" msg="User [s] restored [s] file from [s]"	restore VM license
32206	warning	system	LOG_ID_RESTORE_SCRIPT	user="system" action=restore-script msg="System restored script [s] from management station"	restore script
32207	warning	system	LOG_ID_RETRIEVE_CONF_LIST	user="[s]" ui="[s]" action=retrieve-[s] msg="User [s] failed to retrieve the [s] list from management station"	retrieve configuration list failure
32208	critical	system	LOG_ID_IMPORT_PKCS12_CERT	user="[s]" ui="[s]" action=import-certificate msg="User [s] imported the certificate from [s]"	import the pkcs12 certificate
32209	critical   notice	system	LOG_ID_RESTORE_USR_DEF_IPS	user="[s]" ui="[s]" action=restore-ips-signature status=success msg="Administrator [s] restored the user-defined IPS signatures from [s]"	restore the user-defined IPS signatures
32210	notice	system	LOG_ID_BACKUP_IMG	user="[s]" ui="[s]" action=backup status=success msg="Firmware image backed up to flash disk for system [s]"	backup image
32211	notice	system	LOG_ID_UPLOAD_REVISION	user="[s]" ui="[s]" action=upload status=success msg="User [s] upload the [s] from [s] to flash disk"	upload revision
32212	notice	system	LOG_ID_DELETE_REVISION	action=delete status=success msg="[s]:[n] has been deleted from revision data base"	revision DB deletion

ID	Severity	Subtype	Macro	Format	Description
32213	warning	system	LOG_ID_RESTORE_TEMPLATE	user="system" action=restore-cfg msg="System restored [s] file [s] from management station"	restore template
32214	warning	system	LOG_ID_RESTORE_FILE	user="system" action=restore-[s] msg="System failed to restore [s] file [s] from management station"	restore failure
32215	critical	system	LOG_ID_UPT_IMG	user="[s]" ui="[s]" action=update-image msg="User [s] loaded a wrong image from [s]."	update image
32217	warning   notice	system	LOG_ID_UPD_IPS	user="[s]" ui="[s]" action=update msg="User [s] has updated IPS package by SCP"	An user has updated the IPS package by SCP
32218	warning	system	LOG_ID_UPD_DLP	user="[s]" ui="Fortimanager" action=update msg="User [s] failed to update DLP fingerprint database by SCP"	An user failed to update the DLP fingerprint database by SCP
32219	warning	system	LOG_ID_BACKUP_OUTPUT	user="[s]" ui="[s]" action=backup msg="User [s] backed up the result of batch mode commands by SCP"	An user has backed up the result of standardized error output by SCP
32220	warning	system	LOG_ID_BACKUP_COMMAND	user="[s]" ui="[s]" action=backup msg="User [s] backed up the result of batch mode commands by SCP"	An user has backed up the result of batch mode commands by SCP
32221	warning	system	LOG_ID_UPD_VDOM_LIC	user="[s]" ui="[s]" action=update msg="User [s] has installed VM license by SCP"	An user has installed the VM license by SCP
32222	notice	system	LOG_ID_GLB_SETTING_CHG	user="[s]" ui=[s] field=virtual-domain action=[s] msg="User [s] changed global setting from [s]"	global setting change
32223	error   notice	system	LOG_ID_BACKUP_USER_DEF_IPS	user="[s]" ui=[s] action=backup status=failure msg="Administrator [s] failed to back up the user-defined IPS signatures from [s]"	backup the user-defined IPS signatures failure

ID	Severity	Subtype	Macro	Format	Description
32224	notice	system	LOG_ID_BACKUP_LOG	user="[s]" ui=[s] action=backup msg="User [s] backed up [s] log from [s]"	backup log
32225	notice	system	LOG_ID_DEL_ALL_REVISION	action=delete status=success msg="[s]:revision data base corruption detected, reset."	revision DB clearance
32226	critical	system	LOG_ID_LOAD_IMG_FAIL	user="[s]" ui=[s] action=loaded-image status=failure msg="User [s] loaded a wrong image from [s]."	loaded an image
32240	critical	system	LOG_ID_SYS_USB_MODE	action=reboot status=success msg="System is rebooted and operating in USB mode with configurations loaded from USB (read-only)"	System is operating in USB mode
32252	critical	system	LOG_ID_FACTORY_RESET	user="[s]" ui=[s] action=factory-reset msg="User [s] reset to the factory settings from [s]"	factory reset
32253	critical	system	LOG_ID_FORMAT_RAID	user="[s]" ui=[s] action=format-rebuild-level msg="User [s] formatted the RAID disk from [s]"	config raid
32254	critical	system	LOG_ID_ENABLE_RAID	user="[s]" ui=[s] action=enable-raid msg="User [s] enabled RAID from [s]"	config raid
32255	critical	system	LOG_ID_DISABLE_RAID	user="[s]" ui=[s] action=disable-raid msg="User [s] disabled RAID from [s]"	config raid
32300	notice	system	LOG_ID_UPLOAD_RPT_IMG	user="[s]" ui=[s] status=[s] action=upload-report-image reason="[s]" msg="User '[s]' [s] upload the report image file '[s]' from [s]([s])"	upload the report image file
32301	notice	system	LOG_ID_ADD_VDOM	user="[s]" ui=[s] action=add-vdom msg="Virtual domain [s] is added"	Vdom is added
32302	notice	system	LOG_ID_DEL_VDOM	user="[s]" ui=[s] action=del-vdom msg="Virtual domain [s] is deleted"	Vdom is deleted

ID	Severity	Subtype	Macro	Format	Description
32340	critical	system	LOG_ID_LOG_DISK_UNAVAIL	msg="Log disk is unavailable"	Log disk is unavailable
32341	notice	system	LOG_ID_LOG_DISK_DEFAULT_DISABLED	msg="Disk log status changed to disabled in upgrade process."	disk log status changed
32400	alert	system	LOG_ID_CONF_CHG	user="[s]" ui="[s]" msg="Configuration is changed in the admin session"	config changed
32545	critical	system	LOG_ID_SYS_RESTART	user=none ui=none action=reboot msg="System will reboot due to scheduled daily restart."	System restart
32546	warning	system	LOG_ID_APPLICATION_CRASH	action=crash msg="Pid: [s], application: [s], Firmware: [s], Signal [n] received, Backtrace:[s]"	Application crash
35001	notice	system	LOG_ID_HA_SYNC_VIRDB	msg="HA slave sync virdb([s]) [s]"	HA slave sync virdb
35002	notice	system	LOG_ID_HA_SYNC_ETDB	msg="HA slave sync etdb([s]) [s]"	HA slave sync etdb
35003	notice	system	LOG_ID_HA_SYNC_EXDB	msg="HA slave sync exdb([s]) [s]"	HA slave sync exdb
35004	notice	system	LOG_ID_HA_SYNC_FLDB	msg="HA slave sync fldb([s]) [s]"	HA slave sync fldb
35005	notice	system	LOG_ID_HA_SYNC_IPS	msg="HA slave sync ids([s]) package [s]"	HA slave sync ids package
35007	notice	system	LOG_ID_HA_SYNC_AV	msg="HA slave sync AV([s]) package [s]"	HA slave sync AV package
35008	notice	system	LOG_ID_HA_SYNC_VCM	msg="HA slave sync VCM([s]) package [s]"	HA slave sync VCM package
35009	notice	system	LOG_ID_HA_SYNC_CID	msg="HA slave sync CID([s]) package [s]"	HA slave sync CID package
35010	error	system	LOG_ID_HA_SYNC_FAIL	msg="HA slave sync failed in [n] turns"	HA slave sync failed
36880	warning	system	LOG_ID_EVENT_SYSTEM_MAC_HOST_STORE_LIMIT	msg="Number of detected user devices exceeds limit that can be persistently stored. Detected [n]; can save [n]."	user device data store limit

ID	Severity	Subtype	Macro	Format	Description
37124	error	vpn	MESGID_NEG_I_P1_ERROR	msg="IPsec phase 1 error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s] error_reason="[s]" peer_ notif="[s]"	IPsec phase 1 error log
37125	error	vpn	MESGID_NEG_I_P2_ERROR	msg="IPsec phase 2 error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s] error_reason="[s]"	IPsec phase 2 error log
37126	error	vpn	MESGID_NEG_NO_STATE_ERROR	msg="IPsec no state error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s] error_reason="[s]"	IPsec no state error log
37133	notice	vpn	MESGID_INSTALL_SA	msg="install IPsec SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" role=[s] in_ spi="[s]" out_spi="[s]"	install IPsec SA log
37134	notice	vpn	MESGID_DELETE_P1_SA	msg="delete IPsec phase 1 SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]"	delete IPsec phase 1 SA log
37135	notice	vpn	MESGID_DELETE_P2_SA	msg="delete IPsec phase 2 SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" enc_ spi="[s]" dec_spi="[s]"	delete IPsec phase 2 SA log



ID	Severity	Subtype	Macro	Format	Description
37136	error	vpn	MESGID_DPD_FAILURE	msg="IPsec DPD failure" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s]	IPsec DPD failure log
37137	error	vpn	MESGID_CONN_FAILURE	msg="IPsec connection failure" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s]	IPsec connection failure log
37138	notice	vpn	MESGID_CONN_UPDOWN	msg="IPsec connection status change" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" tunnelip=[s] tunnelid=[n] tunneltype="ipsec" duration=[n] sent=[n] rcvd=[n] nextstat=[n] tunnel="[s]"	IPsec connection status change log
37139	notice	vpn	MESGID_P2_UPDOWN	msg="IPsec phase 2 status change" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" phase2_ name=[s]	IPsec phase 2 status change log
37140	notice	vpn	MESGID_AUTO_IPSEC	msg="auto-ipsec status change" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" status=[s] reason="[s]"	auto-ipsec status log

ID	Severity	Subtype	Macro	Format	Description
37141	notice	vpn	MESGID_CONN_STATS	msg="IPsec tunnel statistics" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" xauthuser="[s]" xauthgroup="[s]" vpntunnel="[s]" tunnelip=[s] tunnelid=[n] tunneltype="[s]" duration=[n] sent=[n] rcvd=[n] nextstat=[n] tunnel="[s]"	IPsec tunnel statistics log
37188	error	vpn	MESGID_NEG_I_P1_ERROR_IKEV2	msg="IPsec phase 1 error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" status=[s] error_reason="[s]"	IPsec phase 1 error log
37189	error	vpn	MESGID_NEG_I_P2_ERROR_IKEV2	msg="IPsec phase 2 error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" status=[s] error_reason="[s]"	IPsec phase 2 error log
37190	error	vpn	MESGID_NEG_NO_STATE_ERROR_IKEV2	msg="IPsec no state error" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" status=[s] error_reason="[s]"	IPsec no state error log
37197	notice	vpn	MESGID_INSTALL_SA_IKEV2	msg="install IPsec SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" role=[s] in_spi="[s]" out_spi="[s]"	install IPsec SA log
37198	notice	vpn	MESGID_DELETE_P1_SA_IKEV2	msg="delete IPsec phase 1 SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]"	delete IPsec phase 1 SA log

ID	Severity	Subtype	Macro	Format	Description
37199	notice	vpn	MESGID_DELETE_P2_SA_IKEV2	msg="delete IPsec phase 2 SA" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" enc_spi="[s]" dec_spi="[s]"	delete IPsec phase 2 SA log
37200	error	vpn	MESGID_DPD_FAILURE_IKEV2	msg="IPsec DPD failure" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" status=[s]	IPsec DPD failure log
37201	error	vpn	MESGID_CONN_FAILURE_IKEV2	msg="IPsec connection failure" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" status=[s]	IPsec connection failure log
37202	notice	vpn	MESGID_CONN_UPDOWN_IKEV2	msg="IPsec connection status change" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" tunnelip=[s] tunnelid=[n] tunneltype="ipsec" duration=[n] sent=[n] rcvd=[n] nextstat=[n] tunnel="[s]"	IPsec connection status change log
37203	notice	vpn	MESGID_P2_UPDOWN_IKEV2	msg="IPsec phase 2 status change" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" phase2_name="[s]"	IPsec phase 2 status change log
37204	notice	vpn	MESGID_CONN_STATS_IKEV2	msg="IPsec tunnel statistics" action=[s] remip=[s] locip=[s] remport=[n] locport=[n] outintf=[s] cookies="[s]" user="[s]" group="[s]" vpntunnel="[s]" tunnelip=[s] tunnelid=[n] tunneltype="[s]" duration=[n] sent=[n] rcvd=[n] nextstat=[n] tunnel="[s]"	IPsec tunnel statistics log

ID	Severity	Subtype	Macro	Format	Description
37888	notice	system	MESGID_HA_GROUP_DELETE	msg="HA group is deleted" ha_group=[n]	HA group delete log
37889	notice	system	MESGID_VC_DELETE	msg="Virtual cluster is deleted" vcluster=[n]	Virtual cluster delete log
37890	notice	system	MESGID_VC_MOVE_VDOM	msg="Virtual cluster's vdom is moved" from_ vcluster=[n] to_vcluster=[n] vdname="[s]"	Virtual cluster move vdom log
37891	notice	system	MESGID_VC_ADD_VDOM	msg="Virtual cluster's vdom is added" to_ vcluster=[n] vdname="[s]"	Virtual cluster add vdom log
37892	notice	system	MESGID_VC_MOVE_MEMB_STATE		Virtual cluster move member state log
37893	notice	system	MESGID_VC_DETECT_MEMB_DEAD	msg="Virtual cluster detected member dead" vcluster=[n] ha_group=[n] sn="[s]"	Virtual cluster detect member dead log
37894	notice	system	MESGID_VC_DETECT_MEMB_JOIN	msg="Virtual cluster detected member join" vcluster=[n] ha_group=[n] sn="[s]"	Virtual cluster detect member join log
37895	notice	system	MESGID_VC_ADD_HADEV	msg="Virtual cluster add HA device" vcluster=[n] devintfname="[s]"	Virtual cluster add HA device(interface) log
37896	notice	system	MESGID_VC_DEL_HADEV	msg="Virtual cluster delete HA device(interface)" vcluster=[n] devintfname="[s]"	Virtual cluster delete HA device(interface) log
37897	notice	system	MESGID_HADEV_READY	msg="HA device(interface) ready" ha_role=[s] devintfname="[s]"	HA device(interface) ready log
37898	warning	system	MESGID_HADEV_FAIL	msg="HA device(interface) fail" ha_role=[s] devintfname="[s]"	HA device(interface) fail log
37899	notice	system	MESGID_HADEV_PEERINFO	msg="HA device(interface) peerinfo" ha_role=[s] devintfname="[s]"	HA device(interface) peerinfo log
37900	notice	system	MESGID_HBDEV_DELETE	msg="Heartbeat device(interface) delete" devintfname="[s]"	Heartbeat device(interface) delete log
37901	critical	system	MESGID_HBDEV_DOWN	msg="Heartbeat device(interface) down" ha_role=[s] hbdn_reason="[s]" devintfname="[s]"	Heartbeat device(interface) down log

ID	Severity	Subtype	Macro	Format	Description
37902	information	system	MESGID_HBDEV_UP	msg="Heartbeat device(interface) up" ha_role=[s] devintfname="[s]"	Heartbeat device(interface) up log
37903	information	system	MESGID_SYNC_STATUS	msg="The sync status with the master" sync_type=[s] sync_status="[s]"	The sync status with the master log
37904	information	system	MESGID_HA_ACTIVITY	msg="HA activity report" ip=[s] ha-prio=[n] activity="[s]"	HA activity report log
38010	alert	user	LOG_ID_FIPS_ENCRY_FAIL	user="[s]" ui=[s] action=encryption cipher=aes-128-cbc status=failed msg="EVP encryption failed"	Encryption failed
38011	alert	user	LOG_ID_FIPS_DECRY_FAIL	user="[s]" ui=[s] action=decryption cipher=aes-128-cbc status=failed msg="EVP decryption failed"	Decryption failed
38012	notice	user	LOG_ID_ENTROPY_TOKEN	user=system action=seeding msg="Seeding PRNG from entropy token"	Seeding from entropy token
38031	notice	user	LOG_ID_FSSO_LOGON	user="[s]" src=[n].[n].[n].[n] server="[s]" action=FSSO-polling-logon status=success reason="[s]" msg="FSSO-polling-logon event from [s]: user [s] logged on [n].[n].[n].[n]"	authentication information
38032	notice	user	LOG_ID_FSSO_LOGOFF	user="[s]" src=[n].[n].[n].[n] server="[s]" action=FSSO-polling-logoff status=success reason="[s]" msg="FSSO-polling-logoff event from [s]: user [s] logged off [n].[n].[n].[n]"	authentication information
38033	notice	user	LOG_ID_FSSO_SVR_STATUS	user="[s]" server="[s]" action=FSSO-polling-AD-server msg="FSSO-polling-AD-server status changes: [s] -> [s]"	authentication information

ID	Severity	Subtype	Macro	Format	Description
38400	notice	system	LOGID_EVENT_NOTIF_SEND_SUCC	user="[s]" from="[s]" to="[s]" service="[s]" proto=[s] dst=[s] dport=[n] nf_type=[s] virus="[s]" profile="[s]" profiletype="[s]" profilegroup="[s]" count=[n] duration=[n] msg="Successfully sent a notification message."	The system successfully sent a notification message log
38401	warning	system	LOGID_EVENT_NOTIF_SEND_FAIL	user="[s]" from="[s]" to="[s]" service="[s]" proto=[s] dst=[s] dport=[n] nf_type=[s] virus="[s]" profile="[s]" profiletype="[s]" profilegroup="[s]" count=[n] duration=[n] msg="Unable to send notification message." sess_duration=[n]	The system was unable to send a notification message log
38402	notice	system	LOGID_EVENT_NOTIF_DNS_FAIL	hostname="[s]" service="[s]" profile="[s]" profiletype="[s]" profile_vd="[s]" msg="Unable to resolve hostname."	The system was unable to resolve an MMSC hostname log
38403	notice	system	LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE	msg="[s] ([s])"	Insufficient resource
38404	notice	system	LOGID_EVENT_NOTIF_HOSTNAME_ERROR	hostname="[s]" msg="[s]"	Unable to resolve FortiGuard hostname
38405	notice	system	LOGID_NOTIF_CODE_SENDTO_SMS_PHONE	user="[s]" action=send-activation-code msg="Send token [s] activation code [s] to [s]"	send activation code
38406	notice	system	LOGID_NOTIF_CODE_SENDTO_SMS_TO	user="[s]" action=send-activation-code msg="Send token [s] activation code [s] to [s]"	send activation code
38407	notice	system	LOGID_NOTIF_CODE_SENDTO_EMAIL	user="[s]" action=send-activation-code msg="Send token [s] activation code [s] to [s]"	send activation code
38408	information	system	LOGID_EVENT_OFTP_SSL_CONNECTED	dst=[n].[n].[n].[n] dstport=[n] action=connect status=success msg="SSL connection to [n].[n].[n].[n] is successfully established."	SSL connection established.

ID	Severity	Subtype	Macro	Format	Description
38409	information	system	LOGID_EVENT_OFTP_SSL_DISCONNECTED	dst=[n].[n].[n].[n] dstport=[n] action=disconnect status=success msg="SSL connection to [n].[n].[n].[n] is successfully closed."	SSL connection closed.
38410	information	system	LOGID_EVENT_OFTP_SSL_FAILED	dst=[n].[n].[n].[n] dstport=[n] reason="[s]([n])" action=connect status=failure msg="SSL read to [n].[n].[n].[n] has failed."	SSL connection failure.
38656	notice	user	LOGID_EVENT_RAD_RPT_PROTO_ERROR	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38657	notice	user	LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38658	notice	user	LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38659	notice	user	LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38660	notice	user	LOGID_EVENT_RAD_RPT_ACCT_EVENT	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38661	notice	user	LOGID_EVENT_RAD_RPT_OTHER	count=[n] duration=[n] msg="[s]"	RADIUS protocol/profile/context error, missing stop packet,accounting or other report log
38662	notice	user	LOGID_EVENT_RAD_STAT_PROTO_ERROR	carrier_ep="[s]" ip=[s] rsoo_key="[s]" msg="[s]" acct_stat=[s] reason="[s]"	RADIUS protocol errors occurred log
38663	notice	user	LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND	carrier_ep="[s]" ip=[s] rsoo_key="[s]" msg="[s]" acct_stat=[s] reason="[s]"	RADIUS start or interim-update packet receivedwith missing or invalid profile specified
38664	notice	user	LOGID_EVENT_RAD_STAT_CTX_NOT_FOUND	carrier_ep="[s]" ip=[s] rsoo_key="[s]" msg="[s]"	RADIUS no context found for user

ID	Severity	Subtype	Macro	Format	Description
38665	notice	user	LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED	carrier_ep="[s]" ip=[s] rso_key="[s]" msg="[s]" acct_stat=[s] reason="[s]"	RADIUS stop packet was missed
38666	notice	user	LOGID_EVENT_RAD_STAT_ACCT_EVENT	carrier_ep="[s]" ip=[s] rso_key="[s]" msg="[s]" acct_stat=[s] reason="[s]"	RADIUS accounting event
38667	notice	user	LOGID_EVENT_RAD_STAT_OTHER	carrier_ep="[s]" ip=[s] rso_key="[s]" msg="[s]" acct_stat=[s] reason="[s]" count=[n]	RADIUS other dynamic profile event
39424	unknown	vpn	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39425	unknown	vpn	LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" duration=[n] sent=[n] rcvd=[n] msg="[s]"	SSL user event log
39426	unknown	vpn	LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39936	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_STATS	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] next_stats=[n] duration=[n] sent=[n] rcvd=[n] msg="[s]"	SSL user event log
39937	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] app-type="[s]" msg="[s]"	SSL user event log
39938	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] app-type="[s]" msg="[s]"	SSL user event log



ID	Severity	Subtype	Macro	Format	Description
39939	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] app-type="[s]" msg="[s]"	SSL user event log
39940	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] app-type="[s]" msg="[s]"	SSL user event log
39941	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39942	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39943	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39944	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_ALERT	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] alert="[s]" desc="[s]" msg="[s]"	SSL user event log
39945	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39946	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR	action="[s]" tunneltype="[s]" tunnel_id=[n] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log

ID	Severity	Subtype	Macro	Format	Description
39947	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39948	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" duration=[n] sent=[n] rcvd=[n] msg="[s]"	SSL user event log
39949	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] next_stats=[n] duration=[n] sent=[n] rcvd=[n] msg="[s]"	SSL user event log
39950	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UNKNOWNTAG	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39951	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39952	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_MODE	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
39953	unknown	vpn	LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_MODE	action="[s]" tunneltype="[s]" tunnel_ id=[n] remote_ip=[s] tunnel_ ip=[s] user="[s]" group="[s]" [s][s][s] reason="[s]" msg="[s]"	SSL user event log
40001	unknown	vpn	LOG_ID_PPTP_TUNNEL_UP	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message

ID	Severity	Subtype	Macro	Format	Description
40002	unknown	vpn	LOG_ID_PPTP_TUNNEL_DOWN	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
40003	unknown	vpn	LOG_ID_PPTP_TUNNEL_STAT	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
40014	warning	vpn	LOG_ID_PPTP_REACH_MAX_CON	status=failure action=connect msg="PPTP: the maximum number of connections has been reached. No more clients can connect."	The maximum number of PPTP connections has been reached
40016	warning	vpn	LOG_ID_L2TPD_SVR_DISCON	action=disconnect status=success reason="interface not found" msg="L2TPD closed all client connections in vdom '[s]' because failed to find interface by device index"	L2TPD disconnection
40017	warning	vpn	LOG_ID_L2TPD_CLIENT_CON_FAIL	action=connect status=failure reason="no ip available" msg="No IP addresses left to assign in virtual domain: [s]"	L2TP client connection
40019	information	vpn	LOG_ID_L2TPD_CLIENT_DISCON	action=disconnect status=success msg="Client [n].[n].[n].[n] control connection (id [n]) finished"	L2TP client disconnection
40021	debug	vpn	LOG_ID_PPTP_NOT_CONIG	status=failure action=connect msg="PPTP: connection request in unconfigured virtual domain: [s]"	pptp is not configured (in this virtual domain)
40022	warning	vpn	LOG_ID_PPTP_NO_IP_AVAIL	status=failure action=connect msg="PPTP: No IP addresses left to assign in virtual domain: [s]"	No ip available
40024	warning	vpn	LOG_ID_PPTP_OUT_MEM	status=failure action=start msg="failed to expand pptp config list due to not enough memory"	Not enough memory

ID	Severity	Subtype	Macro	Format	Description
40034	notice	vpn	LOG_ID_PPTP_START	action=start status=success msg="PPTPD started successfully"	PPTPD start
40035	error	vpn	LOG_ID_PPTP_START_FAIL	action=start status=failure reason="failed to create socket" msg="PPTPD failed to start because failed to create socket"	PPTPD start
40036	notice	vpn	LOG_ID_PPTP_EXIT	action=exit status=success msg="PPTPD exited successfully"	PPTPD exit
40037	information	vpn	LOG_ID_PPTPD_SVR_DISCON	action=disconnect status=success reason="PPTP setting is changed" msg="PPTPD closed all client connections in vdom '[s]' because PPTP setting was changed"	PPTPD disconnect
40038	information	vpn	LOG_ID_PPTPD_CLIENT_CON	action=connect status=success msg="Client [n].[n].[n].[n] control connection started"	PPTPD client connection
40039	information	vpn	LOG_ID_PPTPD_CLIENT_DISCON	action=disconnect status=success msg="Client [n].[n].[n].[n] control connection finished"	PPTPD client disconnection
40101	unknown	vpn	LOG_ID_L2TP_TUNNEL_UP	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
40102	unknown	vpn	LOG_ID_L2TP_TUNNEL_DOWN	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
40103	unknown	vpn	LOG_ID_L2TP_TUNNEL_STAT	action=[s] tunnel_id=[n] [s]tunneltype=[s] remote_ip=[s] tunnel_ip=[s] user="[s]" group="[s]" [s][s][s]msg="[s] [s]"	VPN event log message
40114	notice	vpn	LOG_ID_L2TPD_START	action=start status=success msg="L2TPD started successfully"	L2TPD starting

ID	Severity	Subtype	Macro	Format	Description
40115	notice	vpn	LOG_ID_L2TPD_EXIT	action=exit status=success msg="L2TPD exited successfully"	L2TPD exiting
40118	information	vpn	LOG_ID_L2TPD_CLIENT_CON	action=connect status=success msg="Client [s] control connection started (id [n]), assigned ip [n].[n].[n].[n]"	L2TP client connection
40704	notice	system	LOG_ID_EVENT_SYS_PERF	action="perf-stats" cpu=[n] mem=[n] totalsession=[n] msg="Performance statistics"	system performance log
40960	notice	wad	LOGID_EVENT_WAD_WEBPROXY_FWD_SRV_ERROR	fwserver_name="[s]" addr_ type=[s] ip=[s] fqdn="[s]" port=[n] msg="[s]"	Web proxy forward server error
41000	notice	system	LOG_ID_UPD_FGT_SUCC	[s] msg="Fortigate [s] [s][s][s] [s][s][s] [s][s][s] [s][s][s] [s][s][s] [s][s][s] [s][s][s] [s][s][s] from [s]"	Administrator has updated fortigate successfully
41001	critical	system	LOG_ID_UPD_FGT_FAIL	[s] msg="Fortigate [s] failed"	Administrator has failed to update fortigate
41002	notice	system	LOG_ID_UPD_SRC_VIS	status=update src-vis=yes msg="FortiGate updated src-vis ([s])"	Administrator has updated src-vis plugin successfully
41003	critical	system	LOG_ID_INVALID_UPD_LIC	action=update status=failure msg="HA member [s] does not have valid license"	Invalid update license
41005	notice	system	LOG_ID_UPD_VCM	status=update vcm=yes msg="FortiGate updated VCM ([s])"	Administrator has updated VCM plugin successfully
41984	information	vpn	LOG_ID_EVENT_SSL_VPN_CERT_LOAD	action="[s]" user="[s]" ui="[s]" name="[s]" msg="[s]" cert-type=[s]	Certificate log
41985	information	vpn	LOG_ID_EVENT_SSL_VPN_CERT_REMOVAL	action="[s]" user="[s]" ui="[s]" name="[s]" msg="[s]" cert-type=[s]	Certificate log
41987	information	vpn	LOG_ID_EVENT_SSL_VPN_CERT_UPDATE	action="[s]" cert-type=[s] status="[s]" name="[s]" method="[s]" msg="[s]"	Certificate log
41988	information	vpn	LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE	action="info" user="[s]" ui="[s]" msg="User changed SSL setting"	SSL Setting Updated
41989	information	vpn	LOG_ID_EVENT_SSL_VPN_CERT_ERR	action="[s]" cert-type=[s] status="[s]" name="[s]" method="[s]" msg="[s]"	Certificate log

ID	Severity	Subtype	Macro	Format	Description
41990	information	vpn	LOG_ID_EVENT_SSL_VPN_CERT_UPDATE_FAILED	action="[s]" cert-type=[s] status="[s]" name="[s]" method="[s]" msg="[s]"	Certificate log
43008	notice	user	LOG_ID_EVENT_AUTH_SUCCESS	src=[s] dst=[s] policyid=3 user="user" group="usergroup" ui="HTTP([s])" action=authentication status=success reason="reason" msg="User user succeeded in authentication"	Authentication log
43009	notice	user	LOG_ID_EVENT_AUTH_FAILED	src=[s] dst=[s] policyid=3 user="user" group="usergroup" ui="HTTP([s])" action=authentication status=failure reason="reason" msg="User user failed in authentication"	Authentication log
43010	warning	user	LOG_ID_EVENT_AUTH_LOCKOUT	src=[s] dst=[s] policyid=3 user="user" group="usergroup" ui="HTTP([s])" action=authentication status=locked_out reason="reason" msg="User from [s] was locked out"	Authentication log
43011	notice	user	LOG_ID_EVENT_AUTH_TIME_OUT	src=[s] dst=[s] policyid=[n] user="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="Authentication timed out" msg="[s]"	Authentication log
43012	notice	user	LOG_ID_EVENT_AUTH_FSAE_AUTH_SUCCESS	src=[s] dst=[s] proto=[n] policyid=[n] user="[s]" adgroup="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	FSSO Authentication log
43013	notice	user	LOG_ID_EVENT_AUTH_FSAE_AUTH_FAIL	src=[s] dst=[s] proto=[n] policyid=[n] user="[s]" adgroup="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	FSSO Authentication log
43014	notice	user	LOG_ID_EVENT_AUTH_FSAE_LOGON	src=[s] user="[s]" server="[s]" action=[s] msg="[s]"	FSSO log on/off
43015	notice	user	LOG_ID_EVENT_AUTH_FSAE_LOGOFF	src=[s] user="[s]" server="[s]" action=[s] msg="[s]"	FSSO log on/off

ID	Severity	Subtype	Macro	Format	Description
43016	notice	user	LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS	src=[s] dst=[s] policyid=[n] user="[s]" adgroup="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	NTLM authentication log
43017	notice	user	LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL	src=[s] dst=[s] policyid=[n] user="[s]" adgroup="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	NTLM authentication log
43018	warning	user	LOG_ID_EVENT_AUTH_FGOVRD_FAIL	src=[s] dst=[s] initiator=[s] status=[s] reason="[s]" msg="[s]"	Fortiguard override failed log
43019	warning	user	LOG_ID_EVENT_AUTH_FGOVRD_TBL_FULL	src=[s] dst=[s] initiator=N/A status=failure reason="reason" msg="FortiGuard Web Filtering override table is full"	Fortiguard override log
43020	notice	user	LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS	src=[s] dst=[s] initiator=[s] status=[s] reason="[s]" scope=[s] scope_data="[s]" rule_type=[s] rule_data="[s]" offsite=[s] expiry="[s]" oldwprof="[s]" newwprof="[s]" msg="[s]"	Fortiguard override succeeded log
43021	notice	user	LOG_ID_EVENT_AUTH_ENDPOINT_CHECK	dst=[s] ui="HTTP(0.0.0.0)" msg="forticlient msg"	Endpoint log
43022	notice	user	LOG_ID_EVENT_AUTH_ENDPOINT_LICENSE	dst=[s] ui="HTTP(0.0.0.0)" msg="forticlient msg"	Endpoint log
43023	notice	user	LOG_ID_EVENT_AUTH_ENDPOINT_DET_RECORD	dst=[s] ui="N/A(0.0.0.0)" msg="forticlient msg"	Endpoint log
43024	notice	user	LOG_ID_EVENT_AUTH_ENDPOINT_DET_SESSION	dst=[s] ui="HTTP(0.0.0.0)" msg="forticlient msg"	Endpoint log
43025	notice	user	LOG_ID_EVENT_AUTH_PROXY_SUCCESS	src=[s] dst=[s] policyid=[n] user="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	Wad-auth HTTP log
43026	notice	user	LOG_ID_EVENT_AUTH_PROXY_FAILED	src=[s] dst=[s] policyid=[n] user="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	Wad-auth FTP log
43027	notice	user	LOG_ID_EVENT_AUTH_PROXY_TIME_OUT	src=[s] dst=[s] policyid=[n] user="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="user timed out" msg="[s]"	Wad-auth time out log

ID	Severity	Subtype	Macro	Format	Description
43028	notice	user	LOG_ID_EVENT_AUTH_PROXY_AUTHORIZATION_FAILED	src=[s] dst=[s] policyid=[n] user="[s]" group="[s]" ui="[s]" action=[s] status=[s] reason="[s]" msg="[s]"	Wad-auth HTTP log
43029	notice	user	LOG_ID_EVENT_AUTH_WARNING_SUCCESS	src=[s] dst=[s] initiator=[s] status=[s] reason="[s]" scope=[s] scope_data="[s]" rule_type=[s] rule_data="[s]" offsite=[s] expiry="[s]" oldwprof="[s]" newwprof="[s]" msg="[s]"	Fortiguard override succeeded log
43030	warning	user	LOG_ID_EVENT_AUTH_WARNING_TBL_FULL	src=[s] dst=[s] initiator=[s] status=[s] reason="[s]" msg="[s]"	Fortiguard override failed log
43264	information	system	LOGID_MMS_STATS	proto=[s] infected=[n] suspicious=[n] scanned=[n] intercepted=[n] blocked=[n] checksum=[n] duration=[n]	MMS Statistics log
43520	notice	wireless	LOG_ID_EVENT_WIRELESS_SYS	action="[s]" msg="[s]"	wireless system activity log
43522	notice	wireless	LOG_ID_EVENT_WIRELESS_WTP	sn="[s]" ap="[s]" approfile="[s]" ip=[s] meshmode="[s]" snmeshparent="[s]" action="[s]" reason="[s]" msg="[s]"	physical AP activity log
43524	notice	wireless	LOG_ID_EVENT_WIRELESS_STA	sn="[s]" ap="[s]" vap="[s]" ssid="[s]" user="[s]" group="[s]" mac=[s] ip=[s] channel=[n] radioband="[s]" security="[s]" action="[s]" reason="[s]" msg="[s]"	wireless client activity log
43526	notice	wireless	LOG_ID_EVENT_WIRELESS_WTPR	sn="[s]" ap="[s]" ip="[s]" radioid=[n] configcountry="[s]" opercountry="[s]" cfgtxpower=[n] opertxpower=[n] action="[s]" msg="[s]"	physical AP radio activity log
43527	notice	wireless	LOG_ID_EVENT_WIRELESS_ROGUE_CFG	action="[s]" ssid="[s]" bssid=[s] apstatus=[n] msg="[s]"	wireless rogue AP status config log
43529	notice	wireless	LOG_ID_EVENT_WIRELESS_CLB	sn="[s]" ap="[s]" vap="[s]" ssid="[s]" mac="[s]" radioband="[s]" stacount=[n] action="[s]" reason="[s]" msg="[s]"	wireless client load balancing log



ID	Severity	Subtype	Macro	Format	Description
43530	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC="[s]" manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]"	wireless wids detected log
43532	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC="[s]" manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]"	wireless wids detected log
43533	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC=[s] manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]" Invalidmac=[s]	wireless wids invalid-OUI-detect log
43534	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC=[s] manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]" Dur=[n]	wireless wids long-dur-detect log
43535	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC=[s] manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]" Weakwepiv=[s]	wireless wids weak-wepiv-detect log

ID	Severity	Subtype	Macro	Format	Description
43542	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD	action="[s]" Threattype="[s]" live=[n] TAMAC=[s] manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]" eapoltype=[s] eapolcnt=[n]	wireless wids eapol-packet-flood log
43544	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" TAMAC=[s] manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]" mgmtcnt=[n]	wireless wids mgmt-flood-detect log
43546	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC="[s]" manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]"	wireless wids detected log
43548	notice	wireless	LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP	action="[s]" Threattype="[s]" live=[n] age=[n] channel=[n] rssi=[n] Frametype="[s]" DS="[s]" bssid="[s]" seq=[n] Encrypt=[n] TAMAC="[s]" manuf="[s]" sndetected="[s]" radioiddetected=[n] msg="[s]"	wireless wids detected log
43550	notice	wireless	LOG_ID_EVENT_WIRELESS_STA_LOCATE	sn="[s]" ap="[s]" radioid=[n] radioband="[s]" stamac="[s]" signal=[n] noise=[n] action="[s]" msg="[s]"	wireless station presence detection log
43776	notice	system	LOGID_EVENT_NAC_QUARANTINE	src=[s] dst=[s] src_int=[s] proto=[n] service="[s]" action=[s] user="[s]" group="[s]" policyid=[n] banned_src=[s] banned_ rule="[s]" sensor="[s][n]"	NAC quarantine event log
43800	critical	system	LOG_ID_EVENT_ELBC_BLADE_JOIN	[s]="blade-join" [s]="[n]" [s]="[n]" [s]="[s]" [s]="blade in slot [n] of chassis [n] is ready to process traffic"	blade joins cluster

ID	Severity	Subtype	Macro	Format	Description
43801	critical	system	LOG_ID_EVENT_ELBC_BLADE_LEAVE	[s]="blade-leave" [s]="[n]" [s]="[n]" [s]="[s]" [s]="blade in slot [n] of chassis [n] is no longer ready to process traffic"	blade leaves cluster
43802	critical	system	LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND	[s]="master-found" [s]="[n]" [s]="[n]" [s]="[s]" [s]="blade in slot [n] of chassis [n] became master. there was no previous master."	master blade found
43803	critical	system	LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST	[s]="master-lost" [s]="[n]" [s]="[n]" [s]="[s]" [s]="blade in slot [n] of chassis [n] is no longer master. there is no new master."	master blade lost
43804	critical	system	LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE	[s]="master-changed" [s]="[n]" [s]="[n]" [s]="[n]" [s]="[n]" [s]="[s]" [s]="blade in slot [n] of chassis [n] is no longer master. blade in slot [n] of chassis [n] is the new master"	master blade changed
43805	critical	system	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND	[s]="channel-activate" [s]="[n]" [s]="[n]" [s]="[s]" [s]="[n]" [s]="Channel [n] (FortiSwitch in slot [n]) of chassis [n] became active. there was no previous active channel"	ELBC channel becomes active
43806	critical	system	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST	[s]="channel-deactivate" [s]="[n]" [s]="[n]" [s]="[s]" [s]="[n]" [s]="Channel [n] (FortiSwitch in slot [n]) of chassis [n] became inactive. there is currently no active channel."	ELBC channel becomes inactive
43807	critical	system	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE	[s]="channel-failover" [s]="[n]" [s]="[n]" [s]="[s]" [s]="[n]" [s]="[n]" [s]="Channel [n] (FortiSwitch in slot [n]) of chassis [n] failed over to channel [n] (FortiSwitch in slot [n])."	ELBC channel failover
43808	critical	system	LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE	[s]="chassis-activated" [s]="[n]" [s]="[s]" [s]="chassis [n] became active and will process traffic"	chassis becomes active

ID	Severity	Subtype	Macro	Format	Description
43809	critical	system	LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE	[s]="chassis-deactivated" [s]="[n]" [s]="[s]" [s]="chassis [n] became passive and will not process traffic"	chassis becomes inactive
44288	information	router	LOG_ID_DNS_RESPONSE	policyid=22 src=[s] dst=[s] src_int="eth0" dst_int="switch0" user="user" group="group" dns_name="fotinet dns" dns_ip="1.1.1.1"	test dns event log
44544	information	system	LOGID_EVENT_CONFIG_PATH	user="[s]" ui="[s]" action=[s] cfgtid=[n] cfgpath="[s]" msg="[s]"	config path log
44545	information	system	LOGID_EVENT_CONFIG_OBJ	user="[s]" ui="[s]" action=[s] cfgtid=[n] cfgpath="[s]" cfgobj="[s]" msg="[s]"	config obj log
44546	information	system	LOGID_EVENT_CONFIG_ATTR	user="[s]" ui="[s]" action=[s] cfgtid=[n] cfgpath="[s]" cfgattr=[s] msg="[s]"	config attr log
44547	information	system	LOGID_EVENT_CONFIG_OBJATTR	user="[s]" ui="[s]" action=[s] cfgtid=[n] cfgpath="[s]" cfgobj="[s]" cfgattr=[s] msg="[s]"	config obj attr log
44801	notice	system	44801	limit=[n] msg="[Inbound/Outbound] bandwidth rate exceeded the shaper limit."	[Inbound/Outbound] bandwidth rate exceeded
45000	debug	router	LOG_ID_VSD_SSL_RCV_HS	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive handshake=[s] msg=[s]	SSL handshake received
45001	error	router	LOG_ID_VSD_SSL_RCV_WRG_HS	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive expected=[s] received=[s] msg="Incorrect SSL handshake message"	SSL received incorrect handshake message
45002	debug	router	LOG_ID_VSD_SSL_SENT_HS	serial=[s] policy_id=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=send handshake=[s] msg=[s]	SSL handshake sent

ID	Severity	Subtype	Macro	Format	Description
45003	error	router	LOG_ID_VSD_SSL_WRG_HS_LEN	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive len=[n] msg="Incorrect SSL handshake length"	SSL handshake has invalid length
45004	debug	router	LOG_ID_VSD_SSL_RCV_CCS	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive msg=ChangeCipherSpec	SSL ChangeCipherSpec received
45005	error	router	LOG_ID_VSD_SSL_RSA_DH_FAIL	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="RSA verification of Diffie-Hellman parameters failed"	RSA verification of Diffie-Hellman parameters failed
45006	debug	router	LOG_ID_VSD_SSL_SENT_CCS	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=send msg=ChangeCipherSpec	SSL ChangeCipherSpec sent
45007	error	router	LOG_ID_VSD_SSL_BAD_HASH	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] local=[s] remote=[s] action=close msg="Hash in SSL Finished does not match calculated hash"	Hash in SSL Finished does not match calculated hash
45009	error	router	LOG_ID_VSD_SSL_DECRY_FAIL	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close reason=[n] msg="SSL decryption failure"	SSL decryption failure
45010	debug	router	LOG_ID_VSD_SSL_SESSION_CLOSED	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="SSL session closed"	SSL session closed
45011	error	router	LOG_ID_VSD_SSL_LESS_MINOR	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close min-minor=[n] recv-minor=[n] msg="SSL minor below minimum configured value"	SSL minor version less than configured minimum value

ID	Severity	Subtype	Macro	Format	Description
45012	warning	router	LOG_ID_VSD_SSL_REACH_MAX_CON	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="SSL maximum connections reached"	SSL maximum connection limit reached
45013	error	router	LOG_ID_VSD_SSL_NOT_SUPPORT_CS	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="None of the offered CipherSuites are supported"	None of the offered SSL CipherSuites are supported
45016	debug	router	LOG_ID_VSD_SSL_HS_FIN	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=complete msg="SSL Handshake complete"	SSL handshake complete
45017	error	router	LOG_ID_VSD_SSL_HS_TOO_LONG	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive handshake=[s] len=[n] max=[n] msg="SSL Handshake too long"	SSL handshake too long
45018	debug	router	LOG_ID_VSD_SSL_MORE_MINOR	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=recv max-minor=[n] recv-minor=[n] msg="SSL capping minor version at maximum configured value"	SSL minor version larger than configured maximum value
45019	error	router	LOG_ID_VSD_SSL_SENT_ALERT_ERR	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=send level=[n] desc=[n] msg="SSL Alert sent"	SSL Alert sent
45020	debug	router	LOG_ID_VSD_SSL_SESSION_EXPIRE	vip="[s]" addr=[s] port=[n] created="[s]" id=[s] action=expire msg="SSL session state expired"	SSL session state expiry
45021	debug	router	LOG_ID_VSD_SSL_SENT_ALERT	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=send level=[n] desc=[n] msg="SSL Alert sent"	SSL Alert sent

ID	Severity	Subtype	Macro	Format	Description
45022	debug	router	LOG_ID_VSD_SSL_RCV_CH	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive handshake=ClientHello msg=ClientHello ssl2=[n] major=[n] minor=[n] session_ id="[s]"[s][s][s][s][s]	SSL ClientHello received
45023	debug	router	LOG_ID_VSD_SSL_RCV_SH	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive handshake=ServerHello msg=ServerHello major=[n] minor=[n] cipher=[s] session_id="[s]"[s][s][s]	SSL ServerHello received
45024	debug	router	LOG_ID_VSD_SSL_SENT_SH	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=send handshake=ServerHello msg=ServerHello major=[n] minor=[n] cipher=[s] session_id="[s]"[s][s][s]	SSL ServerHello sent
45025	error   debug	router	LOG_ID_VSD_SSL_RCV_ ALERT	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive level=[n] desc=[n] msg="SSL Alert received"	SSL Alert received
45027	error	router	LOG_ID_VSD_SSL_INVALID_ CONT_TYPE	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=receive type=[n] msg="Invalid SSL ContentType"	Invalid SSL ContentType
45029	error	router	LOG_ID_VSD_SSL_BAD_ CCS_LEN	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="Bad length in SSL ChangeCipherSpec"	SSL ChangeCipherSpec has bad length
45031	error	router	LOG_ID_VSD_SSL_BAD_DH	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] min=[n] max=[n] received=[n] action=close msg="[s]"	SSL Diffie-Hellman has bad value

ID	Severity	Subtype	Macro	Format	Description
45032	error	router	LOG_ID_VSD_SSL_PUB_KEY_TOO_BIG	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] len=[n] max=[n] action=close msg="[s]"	Certificate's public key is too big for SSL offloading
45033	error	router	LOG_ID_VSD_SSL_NOT_SUPPORT_CM	serial=[s] policy=[n] identidx=[n] vip="[s]" src=[s] src-port=[n] dst=[s] dst-port=[n] action=close msg="None of the offered CompressionMethods are supported"	None of the offered SSL CompressionMethods are supported
45056	notice	system	LOG_ID_FCC_EXCEED	action=[s] status=[s] license_limit=[n] reason="[s]" repeat=[n] msg="FortiClient license maximum has been reached."	forticlient license exceed msg
45057	information	system	LOG_ID_FCC_ADD	action=[s] status=[s] license_limit=[s] license_used=[n] used_for_type=[n] connection_type=[s] count=[n] user="[s]" ip=[s] name="[s]" forticlient_id="[s]" msg="Add a FortiClient Connection."	add forticlient connection msg
45058	information	system	LOG_ID_FCC_CLOSE		close forticlient connection msg
45059	notice	system	LOG_ID_FCC_UPGRADE_SUCC	action=[s] status=[s] ui="[s]" user="[s]" license_limit=[s] msg="FortiClient license has been upgraded."	upgrade forticlient license msg
45060	error	system	LOG_ID_FCC_UPGRADE_FAIL	action=[s] status=[s] ui="[s]" user="[s]" reason="[s]" msg="Failed to upgrade FortiClient license."	upgrade forticlient license failed msg
45100	warning	system	LOG_ID_EC_REG_FAIL	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_id=[s] interface=[s] msg="FortiClient registration failed due to blocked UID."	FortiClient registration fail msg
45101	notice	system	LOG_ID_EC_REG_SUCCEED	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_id=[s] interface=[s] msg="FortiClient registration succeeded."	FortiClient registration succeed msg



ID	Severity	Subtype	Macro	Format	Description
45102	notice	system	LOG_ID_EC_REG_RENEWED	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_ id=[s] interface=[s] msg="FortiClient registration renewed."	FortiClient registration renew msg
45103	notice	system	LOG_ID_EC_REG_BLOCK	forticlient_id=[s] msg="FortiClient is blocked for registration."	FortiClient registration block msg
45104	notice	system	LOG_ID_EC_REG_UNBLOCK	forticlient_id=[s] msg="FortiClient is unblocked for registration."	FortiClient registration unblock msg
45105	notice	system	LOG_ID_EC_REG_DEREG	forticlient_id=[s] msg="FortiClient is de-registered."	FortiClient registration de-register msg
45106	notice	system	LOG_ID_EC_REG_LIC_ UPGRADED	msg="FortiClient registration license upgraded."	FortiClient registration license upgrade msg
45107	notice	system	LOG_ID_EC_CONF_ DISTRIBUTED	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_ id=[s] interface=[s] msg="FortiClient configuration distributed."	FortiClient configuration distribute msg
45108	notice	system	LOG_ID_EC_FTCL_UNREG	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_ id=[s] interface=[s] msg="FortiClient unregistered."	FortiClient unregister msg
45109	notice	system	LOG_ID_EC_FTCL_LOGOFF	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_ id=[s] interface=[s] msg="FortiClient logged off."	FortiClient logoff msg
45110	notice	system	LOG_ID_EC_FTCL_ENABLE_ NOTSYNC	user="[s]" hostname="[s]" ip=[n].[n].[n].[n] forticlient_ id=[s] interface=[s] msg="FortiClient SYNC_ WITH_FGT disabled."	FortiClient disable SYNC_ WITH_FGT msg
46000	notice	system	LOG_ID_VIP_REAL_SVR_ENA	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=enable msg="ldb server enabled"	VIP realserver has been enabled.
46001	alert	system	LOG_ID_VIP_REAL_SVR_ DISA	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=disable msg="ldb server disabled"	VIP realserver has been disabled.
46002	notice	system	LOG_ID_VIP_REAL_SVR_UP	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=up msg="ldb server up"	VIP realserver has become up.

ID	Severity	Subtype	Macro	Format	Description
46003	alert	system	LOG_ID_VIP_REAL_SVR_DOWN	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=down msg="ldb server down"	VIP realserver has been down.
46004	notice	system	LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=holddown msg="ldb server entered holddown period" interval=[n](sec)	VIP realserver has started holddown period.
46005	alert	system	LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] action=holddown msg="ldb server health checking failed during holddown period"	VIP realserver has failed holddown.
46006	debug	system	LOG_ID_VIP_REAL_SVR_FAIL	vip="[s]" server=[n].[n].[n].[n] port=[n] status=[s] monitor-name=[s] monitor-type=[s] action=check msg="ldb server health checking failed"	Health monitor has detected VIP realserver health problem.
46084	error	system	LOG_EVENT_REPUTATION_VDOM_PURGE_ERROR	action=reputation_purge status=failure reason="[s]" msg="Failed to complete reputation db maintenance for vdom [s]"	reputation tracking data maintenance
46085	information	system	LOG_EVENT_REPUTATION_VDOM_PURGE_SUCCESS	action=reputation_purge status=success msg="Completed reputation db maintenance"	reputation tracking data maintenance
46092	information	system	LOG_EVENT_REPUTATION_ERASE_DATA_ERROR	action=reputation_clear status=failure reason="[s]" msg="Failed to erase reputation db for vdom [s]"	reputation report
46093	information	system	LOG_EVENT_REPUTATION_ERASE_DATA_SUCCESS	action=reputation_clear status=success msg="Erased reputation db for vdom [s]"	reputation report
47201	emergency	system	LOG_ID_AMC_ENTER_BYPASS	msg="The AMC card in slot [s] has entered bypass mode due to [s]."	AMC card entered bypass mode
47202	emergency	system	LOG_ID_AMC_EXIT_BYPASS	msg="The AMC card in slot [s] has exited bypass mode due to [s]."	AMC card exited bypass mode
47203	emergency	system	LOG_ID_ENTER_BYPASS	msg="The bypass ports pair have entered bypass mode."	Bypass ports pair entered bypass mode

ID	Severity	Subtype	Macro	Format	Description
47204	emergency	system	LOG_ID_EXIT_BYPASS	msg="The bypass ports pair have exited bypass mode."	Bypass ports pair exited bypass mode
48000	debug	wad	LOG_ID_WAD_SSL_RCV_HS	session_id=[s] policyid=[n] src=[n].[n].[n].[n] srcport=[n] dst=[n].[n].[n].[n] dstport=[n] action=receive handshake="[s]"	SSL handshake received
48001	error	wad	LOG_ID_WAD_SSL_RCV_WRG_HS	session_id=[s] policyid=[n] src=[n].[n].[n].[n] srcport=[n] dst=[n].[n].[n].[n] dstport=[n] action=receive msg="Incorrect SSL handshake length. len:[n]"	SSL handshake has invalid length